

---

# **Universidad de Valladolid**

*Facultad de Derecho*

*Grado en Criminología*

***Tecnología de vigilancia, seguimiento y  
localización de objetivos***

Presentado por:

***Emilia Inés Bernal García***

Tutelado por:

***Dra. D<sup>a</sup>. Beatriz Sainz de Abajo***

Valladolid, junio de 2019

## Reconocimiento-No comercial-Sin obras derivadas.



### Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra, **bajo las condiciones siguientes:**
- **Reconocimiento:** debe reconocer los créditos de la obra de la manera especificada por el autor, pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra;
- **No comercial:** no puede utilizar esta obra para fines comerciales;
- **Sin obras derivadas:** no puede alterar, transformar o generar una obra derivada a partir de esta obra.
- Si reutiliza o distribuye esta obra, tiene que dejar bien claro los términos de la licencia.
- alguna de estas condiciones puede no aplicarse si obtiene el permiso del titular de los derechos de autor.
- Esta licencia no menoscaba ni restringe los derechos morales del autor.

TITULO: Tecnología de vigilancia, seguimiento y localización de objetivos

AUTORA: D<sup>a</sup>. Emilia Inés Bernal García

TUTORA: Dra. D<sup>a</sup>. Beatriz Sainz de Abajo

**COMISIÓN EVALUADORA:**

PRESIDENTE: Dra. D<sup>a</sup>. Beatriz Sainz de Abajo

VOCAL 1: Dr. D. Miguel López-Coronado Sánchez-Fortún

VOCAL 2: Dra. D<sup>a</sup>. Isabel de la Torre Díez

SUPLENTE 1º: Dr. D. Carlos Gómez Peña

SUPLENTE 2º: Dr. D. Jesús Poza Crespo

SUPLENTE 3º: Dra. D<sup>a</sup>. María García Gadañón

**CONVOCATORIA:** JUNIO 2019

## **RESUMEN**

La tecnología moderna que se emplean hoy día para realizar vigilancia y seguimiento está a la orden del día. En este documento se describen los dispositivos destinados a estos fines, muchos de ellos a nuestro alcance. En cada apartado se informa de los usos principales y su marco normativo.

## **ABSTRACT**

Currently, modern technology for surveillance and monitoring is the order of the day. This document describes the devices designed for these purposes, many of them within our reach. In each section, the main uses and their normative framework are reported.

## **PALABRAS CLAVE**

Tecnología, vigilancia, seguimiento, localización, satélite, imagen, Internet

## **KEYWORDS**

Technology, surveillance, tracking, location, satellite, image, internet

**Agradecimientos:**

A mi padre, ausente, pero siempre presente. A mi madre por ser ella.

A mi marido y a mi hijo por su inspiración, y por enseñarme el valor de la familia.

Agradecer también a mi tutora, D<sup>a</sup> Beatriz Sainz de Abajo, por su apoyo y disponibilidad.

## INDICE

1. INTRODUCCIÓN.....	9
2. TECNOLOGÍAS DE VIGILANCIA.....	12
2.1. Aproximación al concepto.....	12
2.2. Clasificación.....	12
2.2.1. Cámaras de vigilancia.....	12
2.2.1.2. Categorías de cámaras de vigilancia.....	13
2.2.2. Micrófonos.....	15
2.2.2.1. Con tecnología GSM.....	15
2.2.2.2. Inalámbricos.....	16
2.2.2.3. De pared.....	16
2.2.2.4. Telefónicos.....	16
2.2.3. Globo aerostático.....	16
2.2.4. Dron.....	17
2.2.5. Radar.....	18
2.2.6. Satélite artificial.....	19
2.2.6.1. Climáticos.....	19
2.2.6.2. De comunicación.....	20
2.2.6.3. De televisión.....	20
2.2.6.4. Científicos.....	20
2.2.6.5. De navegación.....	20
2.2.6.6. De rescate.....	20
2.2.6.7. De observación.....	20
2.2.6.8. Militares.....	20
2.3. Usos.....	21
2.3.1. De las cámaras de vigilancia.....	21
2.3.2. De los micrófonos.....	22
2.3.3. De los globos aerostáticos.....	22

2.3.4. Del dron .....	23
2.3.5. Del radar.....	23
2.3.6. Del satélite.....	23
2.4. Marco normativo.....	24
3. TECNOLOGÍAS DE SEGUIMIENTO.....	28
3.1. Aproximación al concepto .....	28
3.2. Clasificación .....	28
3.2.1.-Smartphones y Apps .....	28
3.2.2. Tableta .....	29
3.2.3. Wearables devices .....	29
3.2.4. Big data.....	30
3.2.5. Redes sociales .....	31
3.2.6. Tecnología de seguimiento de usuarios de internet.....	32
3.2.6.1. Cookies y cookies flash.....	32
3.2.6.2. Balizas Web.....	32
3.2.6.3. Píxeles de seguimiento .....	33
3.2.6.4. Browser Fingerprint Tracker.....	33
3.2.6.5. Interfaces.....	33
3.2.7. Internet of things (IoT).....	34
3.2.8. Tecnologías de Información y Comunicación (TIC).....	34
3.3. Usos .....	35
3.4. Legislación .....	37
4. TECNOLOGÍAS DE LOCALIZACIÓN.....	40
4.1. Aproximación al concepto .....	40
4.2. Clasificación .....	40
4.2.1. Sistemas de posicionamiento por satélite .....	40
4.2.1.1. GPS.....	40

4.2.1.2. GLONASS.....	41
4.2.1.3. Galileo .....	42
4.2.1.4. Otros satélites a considerar.....	43
4.2.2. Geolocalización.....	43
4.2.3. Localización GSM.....	44
4.2.4. Tecnologías de localización LBS y Localización en Tiempo Real (RTLS).....	45
4.2.4.1. Visible Light Communication (VLC).....	46
4.2.4.2. Sensores inerciales .....	46
4.2.4.3. Ultrasonido .....	47
4.2.4.4. Bluetooth Low Energy (BLE).....	47
4.2.4.5. Wi-Fi.....	48
4.2.4.6. Ultrawideband (UWB) .....	48
4.2.4.7. Radio Frecuency Identification (RFID) .....	49
4.2.4.8. Zigbee.....	50
4.3. Usos .....	51
4.4. Legislación.....	53
5. CONCLUSIONES.....	55
6. REFERENCIAS BIBLIOGRÁFICAS .....	57
7. ACRÓNIMOS .....	64
ANEXOS .....	65

# 1. INTRODUCCIÓN

Los sistemas tecnológicos de vigilancia electrónica han evolucionado en los últimos tiempos. Lo que antes veíamos en las películas como ciencia ficción se está convirtiendo poco a poco en realidad. Estos equipos se han desarrollado para proporcionar apoyo a las investigaciones que requieren el uso de micrófonos ocultos, cámaras y dispositivos de localización para recopilar información a través de la vigilancia de personas y lugares. Resultan especialmente útiles en el seguimiento de personas desaparecidas o el seguimiento de vehículos por medio de dispositivos de monitoreo satelital.

Los gobiernos se valen de estos medios para la lucha contra el crimen organizado, el terrorismo y la información militar, para lo que no escatiman medios económicos que permitan el desarrollo de estas tecnologías.

Países como China están a la vanguardia en técnicas de identificación de personas. Otros, como Estados Unidos, estudian la forma de adaptar tecnologías de reconocimiento facial en 3D e implementarlas al sistema satelital para llegar a localizar a una persona en cualquier parte del mundo, todo ello a la vez que desarrollan bases de datos para contrastar la información recibida.

Al mismo tiempo, la sociedad de consumo en que vivimos hace que invirtamos en dispositivos como smartphones, tablets y watches que permiten que seamos predecibles y localizables prácticamente en cualquier momento.

Otras veces, nos exponemos y ofrecemos información personal y de fácil seguimiento a través de las redes sociales, información personal que queda disponible en algún lugar de la nube digital, pudiendo ser accesible ante cualquiera.

El mundo está influenciado e hipnotizado por las novedades tecnológicas. Lo nuevo hoy, queda obsoleto en pocos años. Con esto, se abre un modo evolutivo delincencial, puesto que no sólo las nuevas tecnologías son útiles para el usuario tipo, sino que el criminal también se puede servir de estos avances para ejecutar sus acciones, por lo que se constituye un factor más para que el criminólogo amplíe sus conocimientos en aras de la prevención general.

La criminología es una ciencia multidisciplinar que estudia el crimen, la criminalidad derivada de la comisión de delitos y conductas antisociales para así conocer cómo evitar comportamientos negativos de estas conductas en la sociedad. Para un criminólogo es necesario y fundamental estar a la vanguardia de estas tecnologías. Conocer los nuevos dispo-

sitivos y la manera en que pueden ser utilizados, para poder estructurar los mecanismos de prevención que les pudieran ser solicitados.

Desde esta perspectiva, las tecnologías de vigilancia, seguimiento y localización de objetivos deberían de ser un valor al alza para los sistemas públicos por el sentido garantista que resulta para los estados el contar con ellas, al servicio de la resolución de hechos delictivos.

No debemos olvidar que estos avances, además de para la criminología, han tenido una fundamental incidencia y repercusión para la medicina moderna con el monitoreo de pacientes y sus dolencias, y en la comunicación instantánea que ofrece para con los servicios médicos que pueden intervenir en caso de emergencia gracias ellas.

En la sociedad en que vivimos resulta, cuanto menos, emocionante el observar en medios de comunicación cómo se ha encontrado a un desaparecido, cómo se ha localizado un culpable que permanecía oculto, cómo se ha podido hacer la reconstrucción de un caso que mantenía en vilo a la opinión pública...El efecto beneficioso que se obtiene cuando se utilizan estos medios tecnológicos de manera proporcional, necesaria e idónea.

Es por la gran cantidad de conceptos existentes sobre esta materia por lo que he estructurado el presente trabajo en tres partes diferenciadas, en las que se definen los conceptos, para conocer que son y cómo funcionan, desde lenguaje comprensible evitando tecnicismos propios de otras áreas de estudio.

Consta este trabajo de una primera parte en la que establezco una clasificación de sistemas que se utilizan principalmente para la vigilancia, realizado una breve descripción de cada elemento, elaborando un apartado en el que se desarrollan los principales usos de los mismos, y otro final en el que se encuadran las normativas que permiten que puedan ser utilizados y con qué restricciones.

Una segunda parte en la que se hace mención a tecnologías de seguimiento que se vienen utilizando en la actualidad, y en qué ámbitos es más frecuente poder contar con ellas.

Una tercera en la que se definen tecnologías de localización de objetos y personas, así como las principales condiciones de utilización y la normativa de aplicación que la afecta.

En cualquier caso, todas estas tecnologías pueden funcionar de forma relacionada y conjunta, o de forma independiente unas de otras, según la finalidad para la que sean destinadas y el motivo para el que sean elegidas.

Al final, un apartado dedicado a las conclusiones de este proyecto, con una visión de conjunto que acompaña las ideas principales que en este trabajo se han desarrollado.

Por último, un anexo en el que he incluido cuatro noticias de prensa diferenciadas en las que se refleja cómo se utilizan actualmente estas tecnologías por las Fuerzas y Cuerpos de Seguridad.

## 2. TECNOLOGÍAS DE VIGILANCIA

### 2.1. Aproximación al concepto

Podrían definirse como aquellos sistemas o aparatos dotados con tecnologías ya existentes y otras nuevas y más actuales que se vienen utilizando para observar todo aquello perceptible ya sean personas, lugares o cosas, tanto en el ámbito público, desde un campo policial o gubernamental, como en el ámbito privado.

Con su uso, nos permiten mejorar los tiempos de respuesta para promover conductas seguras y ordenadas, no constituyendo solamente una función preventiva.

Por ello, son herramientas de apoyo a las autoridades en su respuesta inmediata ante conductas fuera de norma... o así deberían de serlo.

El “ojo que todo lo ve” genera en la población dos corrientes de opinión totalmente opuestas: por un lado, la confianza y pensamiento positivo en los sistemas de vigilancia, y por otro lado, la convicción de que se produce vulneración de la intimidad.

### 2.2. Clasificación

#### 2.2.1. Cámaras de vigilancia

Son definidas como dispositivos que registran o capturan imágenes fijas o en movimiento y que transmiten las señales captadas.

Es frecuente encontrar este tipo de equipos localizados casi por todas partes: en cajeros automáticos, en carreteras, en establecimientos públicos, en zonas estratégicas de algunas ciudades...estableciendo así un control de todo aquello al alcance de la óptica de sus objetivos. Pueden ser tecnologías de vigilancia terrestre, aérea o marítima



Figura 1: Cámara de Seguridad instalada en Málaga (Fuente: Periódico [LaopiniondeMálaga.es](http://LaopiniondeMálaga.es) Junio 2018)

### 2.2.1.1. Tipos de cámara de vigilancia

#### *Cámaras IP*

Son las cámaras de vigilancia más utilizadas en la actualidad, por la facilidad y fiabilidad que aportan. Estas cámaras transmiten la información a través de una red informática conectada a internet, bien por cable Ethernet, bien por conexión inalámbrica (WiFi). Las imágenes pueden consultarse en tiempo real desde un dispositivo remoto, incluso desde cualquier parte si se tiene un pc, Tablet o Smartphone. También se permite el control de la cámara (dirección de la óptica, así como ampliación o reducción del zoom de visión, inicio de grabación, etc.) mediante estos dispositivos.

#### *Cámaras analógicas*

Serán definidas como aquellas que transmiten la información a través de un cable coaxial hasta un monitor donde se reproduce la imagen. La imagen que se retransmite podrá ser grabada en un registrador digital o memoria.

### 2.2.1.2. Categorías de cámaras de vigilancia

#### *Cámaras térmicas*

También conocidas como Infrarrojas, son aquellas capaces de medir el calor que desprende un cuerpo sin que exista contacto.

Sabemos que los cuerpos emiten calor (radiación infrarroja), lo transmiten e incluso lo reflejan en otros cuerpos. Así, estos dispositivos dotados de sensores que trabajan en un rango que permite la detección del calor, son capaces de generar una imagen del cuerpo u objeto que buscamos y mostrarlos en la pantalla. A cada rango percibido se le asignará un color concreto, con lo que se posibilita la percepción de la imagen.

En modelos de detección de imagen a largo alcance, se incluye un sensor láser que percibirá cualquier movimiento antes del inicio de grabación de la imagen.

Además de usos industriales y de construcción, estas cámaras se utilizan con éxito para detectar seres vivos en situaciones de emergencia (desprendimientos, terremotos), en situaciones de seguridad (pasos fronterizos) análisis médicos no invasivos, y vienen siendo bastante utilizadas en vigilancias en la oscuridad, pues permiten detectar intrusos a larga distancia de forma tan efectiva y discreta, en prácticamente cualquier condición meteorológica, incluso con lluvia, nieve, niebla o humo.



Figura 2: Cámara térmica-infrarrojos localiza víctimas de agresión en Boston (fuente Line Police Boston)<sup>1</sup>

### *Cámaras de reconocimiento facial*

Son aquellas dotadas de un software de reconocimiento facial, a través del cual se permite la identificación de una persona (el reconocimiento del individuo a través de su cara) analizando las características biométricas de su rostro.

Será necesario contar con una base de datos previa para poder realizar la identificación. El funcionamiento de éste software sería el siguiente:

Se detecta y captura el rostro de los individuos al alcance del dispositivo (cámara)

El programa cotejará y conformará el patrón biométrico facial (forma de ojos, separación de cejas, simetrías y asimetrías de esa cara)

La información resultante se contrasta con la existente en la base de datos.

Se identifica el rostro que contenga mayor porcentaje de similitudes de un umbral muy elevado de coincidencia. Para ello se están implementando sistemas de aprendizaje inteligente que funcionarían como algoritmos únicos que combinan un método de aprendizaje automático con un método de cálculo de similitud que suprime los errores.

Si bien es un sistema de vigilancia de gran importancia para Fuerzas de Seguridad y Servicios de inteligencia de Países, diferentes empresas de telefonía e informática vienen desarrollando sus propios programas y aplicaciones que emplean esta tecnología. (por

---

<sup>1</sup> <https://www.20minutos.es/videos/internacional/aflBDKU9-hallan-una-victima-de-violacion-con-una-camara-termica/>.

ejemplo, el Face Id de Apple, o el FaceNet de google- éste último reconocido como inteligencia artificial de Google que implementa el reconocimiento de caras familiares en sus cámaras de seguridad de uso doméstico, manteniendo la base de datos de esas caras en “la nube”, creándose las consiguientes dudas a nivel de seguridad, por este motivo-)

En contra: ¿Es eficaz este sistema de reconocimiento? ¿Cómo funcionaría en eventos como el carnaval en el que las personas se disfrazan o llevan máscaras? Posiblemente no nos permitiría una identificación. Habría que recurrir a otros medios.

#### *Cámaras de reconocimiento de movimiento*

De nuevo el gigante asiático chino sorprende por su vigilancia extrema, al instalar en un colegio de un sistema de video-vigilancia capaz de reconocer los movimientos de sus estudiantes y catalogarlos con la finalidad de mejoras en el sistema docente y para valorar cómo se sienten sus estudiantes, o al menos, eso es lo que afirma el director del centro educativo

Es un sistema de software combinado con reconocimiento facial. Al mismo tiempo define los movimientos, la cadencia y frecuencia de los mismos empleando nuevamente patrones biométricos que designan a quien pertenecen.

En cuanto al reconocimiento de “objetos en movimiento”, existen dispositivos de video-vigilancia que se activan al detectar algo moverse en el radio de su alcance

#### *2.2.2. Micrófonos*

Son traductores electro-acústicos, es decir, dispositivos que transforman la energía acústica en energía eléctrica. Capturan el sonido y permiten que éste se transmita a un altavoz, auricular o a un aparato receptor.

El sonido retransmitido podrá ser grabado para su posterior reproducción.

Existen micrófonos para determinadas cámaras de vigilancia, haciendo posible la edición de audio-video.

Otros micrófonos se emplean exclusivamente para grabaciones y escuchas, existiendo diferentes variantes:

##### *2.2.2.1. Con tecnología GSM*

Son aquellos que llevan tarjeta SIM, y dotados de tecnología cuatribanda. Al detectar movimientos o sonido, llaman a nuestro teléfono móvil, pudiendo escuchar en tiempo

real la conversación que se esté manteniendo en un radio varios metros de distancia de la colocación del micrófono.

#### *2.2.2.2. Inalámbricos*

Cuyo alcance de recepción supera los 100 metros, no llevan cableado.

#### *2.2.2.3. De pared*

Amplifican la señal de audio (por la acción de estetoscopios) al ampliar las vibraciones que se perciben.

#### *2.2.2.4. Telefónicos*

Se alimentan de la línea telefónica.

### *2.2.3. Globo aerostático*

Se trata de un sistema de vigilancia aérea combinado de globo de helio con cable capaz de elevarse a más de 600 metros de altura, con sistema de video-cámaras de vigilancia de transmisión IP (generalmente cámara de visión 360° y térmica) y de un radio de varios kilómetros de alcance (sistemas como el israelí SkyStar, permite visión de hasta 20 kilómetros de distancia y vuelos de 1000 metros de altura con autonomía de una semana)<sup>2</sup>. Son más económicos que los radares, puesto que no necesitan disponer de una estación fija, sino que son fijados a tierra por un cable de acero que lo dirige y evita la pérdida del equipo por elevación extrema o corrientes de aire y, además, es el que suministra la energía y alimentación de los equipos durante unos tres días. Todo el sistema está conectado a una unidad de monitoreo que permite controlar la presión del globo, el peso que lleva la unidad, la tensión del cable que lo dirige, etc.

---

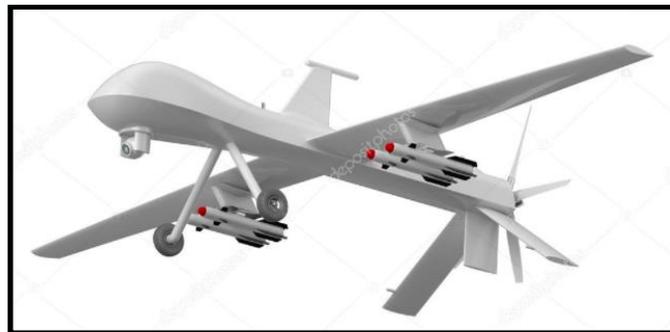
<sup>2</sup> <https://www.hispantv.com/noticias/oriente-medio/283399/israel-globo-espia-rt-lta-skystar> (Consulta 31 de Enero 2019)



*Figura 3: Winch Aerostat Swal Platform*<sup>3</sup>

#### 2.2.4. Dron

Aparato volador NO tripulado, Vehículo Aéreo No Tripulado (VANT) o comúnmente DRON<sup>4</sup> que será controlado de forma remota. Forma parte de los sistemas de vigilancia aérea, y permiten tener referencias visuales de zonas de difícil acceso para el ser humano, puesto que se les dota de videocámara en sus vuelos. Los veremos en acción en maniobras militares, periodísticas, de vigilancia y rescate.



*Figura 4: Military Predator Drone*

---

<sup>3</sup> Fuente: droneaviationcorp.com

<sup>4</sup> 23.<sup>a</sup> Edición del diccionario de la lengua española. Espasa.

Clase (MTOW)	Categoría	Empleo	Altitud de operación AGL	Radio de Misión
CLASE I ≤ 150 Kg	MICRO < 2 Kg	Táctico, (Sección)	Hasta 200 pies	5 Km (LOS)
	MINI 2-20 Kg	Táctico (Compañía)	Hasta 1.000 pies	25 Km (LOS)
	LIGEROS > 20 Kg	Táctico (Batallón)	Hasta 1.200 pies	50 Km (LOS)
CLASE II ≤600 Kg	TÁCTICO	Táctico (Brigada)	Hasta 10.000 pies	200 Km (LOS)
CLASE III > 600 Kg	MALE (Medium Altitude Long Endurance)	Operacional	Hasta 45.000 pies	Sin Limite (BLOS)
	HALE (High Altitude Long Endurance)	Estratégico	Hasta 65.000 pies	Sin Limite (BLOS)
	Combate	Estratégico	Hasta 65.000 pies	Sin limite (BLOS)

Figura 5: Clasificación DRON OTAN<sup>5</sup>

### 2.2.5. Radar

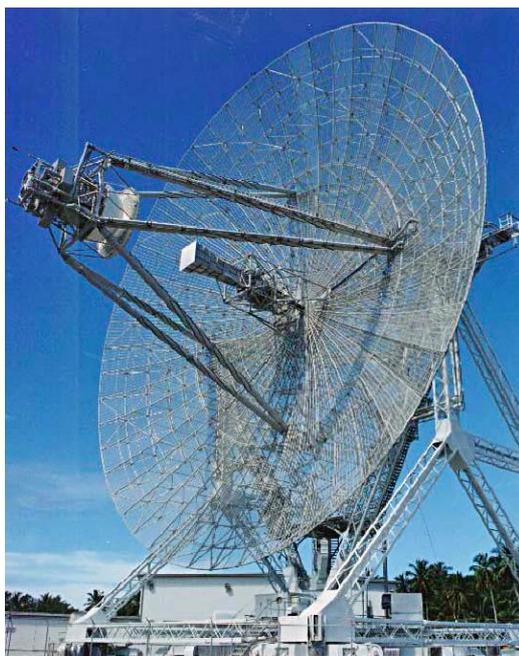
Sistema que utiliza ciertas frecuencias de ondas electromagnéticas para medir distancias, velocidades, direcciones de objetos que están estáticos o en movimiento. Lo hace enviando una señal de radio que se reflejará en el objetivo, el cual rebota la señal que será recibida por el emisor (radar). Es a través d ese “eco” como se recibe la información que se busca.

Radar, proviene del acrónimo ingles cuyo significado es *Radio Detection and Ranging*.

La variabilidad de longitudes de onda que se usan en estos aparatos son las que determinan el tipo de objeto a detectar.

Sus usos principales son en aeropuertos, en geología, en meteorología, cartografías y medioambiental en general, si bien son muy demandados militarmente para defensa y policialmente para vigilancia tanto marítima como terrestre y aérea.

<sup>5</sup> Fuente JCGUAS “UAV Classification Guide”. NNAG. Septiembre 2011 (Consulta 26 enero 2019)



*Figura 6: Radar (fuente Wikipedia)<sup>6</sup>*

#### *2.2.6. Satélite artificial*

Es un aparato creado por el hombre que es lanzado al espacio para permanecer en órbita alrededor de la Tierra y de otros planetas o satélites naturales.

Hay dos grandes categorías de satélites: los de observación (reciben, procesan y transmiten datos desde y hacia la tierra), los de comunicación (transmiten y diseminan la información de unos lugares de la tierra a otros) y dentro de éstos, según su utilidad, los clasificaremos como sigue:

##### *2.2.6.1. Climáticos*

Usados para la predicción del clima, como el conocido METEOSAT (satélite europeo construido por las empresas de tecnología aeroespacial francesas Aérospatiale, Cannes Mandelieu Space Center, Matra, la alemana MBB, la italiana Alenia Aeronautica, y la británica Marconi Company), y que realizan fotografías sobre la capa atmosférica que envían al receptor en la Tierra.

---

<sup>6</sup> Wikipedia, la enciclopedia libre (radar) 2013, disponible en [https://es.wikipedia.org/wiki/Radar#/media/File:Radar\\_antenna.jpg](https://es.wikipedia.org/wiki/Radar#/media/File:Radar_antenna.jpg) (Consulta 26 enero 2019)

#### *2.2.6.2. De comunicación*

Aquellos que realizan envío de datos y conversaciones telefónicas gracias a un aparato que transmite y responde a la señal, denominado transpondedor.

#### *2.2.6.3. De televisión*

Serán aquellos encargados de emitir y enviar la señal de televisión, incluso en directo.

#### *2.2.6.4. Científicos*

Investigan fenómenos naturales y realizan misiones científicas. Es posible observar incluso un incendio y situarlo en el lugar concreto donde se esté produciendo.

#### *2.2.6.5. De navegación*

Hoy en día puestos a disposición civil, gracias por ejemplo, al GPS (*Global Positioning System*) desarrollado por EEUU, que permite la navegación al ser un sistema de posicionamiento.

#### *2.2.6.6. De rescate*

Reciben señales de emergencia de vehículos o naves que así lo transmiten. En la actualidad, existe un sistema denominado eCall, instalado en vehículos nuevos (a partir de abril de 2018 en Europa) que funcionará transmitiendo señal de emergencia en caso de siniestro y mediante antena y satélite. Así, los servicios de rescate pueden actuar con mayor celeridad.

#### *2.2.6.7. De observación*

Aquellos encargados de informar de cambios de consideración que se estén produciendo en la esfera terrestre, como glaciaciones, cambios en la capa de ozono, etc.

#### *2.2.6.8. Militares*

Satélites muy sofisticados que mantienen información reservada a cerca de las investigaciones que realizan sobre operaciones militares, de inteligencia y de comunicaciones.



Figura 7: Satélite NAVSTAR, del sistema GPS (Fuente: [youboit.com](http://youboit.com))<sup>7</sup>

## 2.3. Usos

### 2.3.1. De las cámaras de vigilancia

Como se ha ido observando a lo largo del proceso descriptivo de los diferentes sistemas de cámaras de vigilancia, estas se aplicarán principalmente como mecanismos de control directo o indirecto.

Control directo en el sentido de la información percibida por el ciudadano, por ejemplo, el Ayuntamiento de Málaga en su página web, sección de Movilidad, anuncia la colocación de cámaras de vigilancia de tráfico, así como su sectorización en los diferentes distritos<sup>8</sup>

En este caso, la población conoce de los lugares donde pueden ser detectadas infracciones derivadas de la circulación al haber sido instaladas las cámaras de vigilancia, y actuar en consecuencia. Aquí, las cámaras tienen una función principalmente preventiva.

El control será indirecto, cuando las cámaras sirvan para identificar hechos presuntamente delictivos, vandálicos o fuera de norma, al ser detectados por las cámaras que están colocadas con otra finalidad, pero que de manera “indirecta” perciben todo aquello que ocurre en espacios públicos, incluyendo personas, animales, vehículos y cualquier actuación derivada de los mismos. Quiero decir con ello que, aunque exista una cámara instalada para una función concreta y determinada inicialmente, podría ser de utilidad cualquier imagen que quede grabada si se produjere un hecho de relevancia

---

<sup>7</sup> <https://www.youboit.com/es/article/shared-information/15589/que-son-los-satelites-artificiales-y-como-funcionan>, (consulta 27 Enero 2019)

<sup>8</sup> Ayuntamiento de Málaga <http://movilidad.malaga.eu/es/servicios/camaras-de-trafico/> (Consulta 30 Enero 2019)

ajeno al destinado. Podrían usarse esas imágenes por las autoridades Policiales y Judiciales si así lo requieren.

Las modalidades de reconocimiento facial o de reconocimiento de movimiento están siendo usadas por el gobierno y autoridades policiales, principalmente en países como China o Estados Unidos para la identificación y consecuente vigilancia de personas concretas. En estos casos, las fuerzas del orden y los gobiernos actuarán contrastando las imágenes recibidas con las de sujetos previamente identificados e incluidos en dichas bases de datos.

Las cámaras infrarrojas observarán donde el ojo humano no pueda ver. Utilizadas para vigilancias nocturnas, evitan movimientos fronterizos clandestinos y tráfico de drogas en las funciones de vigilancias de los cuerpos de Policía y Guardia Civil y para la prevención de delitos.

También en maniobras militares y control de perímetros de zonas de seguridad podremos encontrar estos dispositivos.

### *2.3.2. De los micrófonos*

En cuanto a los micrófonos, decir que se trata de uno de los sistemas de vigilancia que más se mantiene en el tiempo. La famosas “escuchas” que tanta relevancia tienen en el sistema jurídico español y que vienen siendo determinantes para la resolución de hechos delictivos y enjuiciamiento de sus culpables desde hace décadas. Además, son pieza clave en espionaje militar e industrial.

### *2.3.3. De los globos aerostáticos*

Ya se ha comentado el hecho de que los globos aerostáticos son sistemas de vigilancia más económicos que los radares por las características descritas con anterioridad. Se utilizan en espionaje militar, para control y vigilancia del tráfico de drogas e incluso para la prevención de ataques terroristas <sup>9</sup> y se han autorizado en algunos países (pese a denuncias emitidas por atentar contra la intimidad) como medida de vigilancia masiva para reforzar los planes de seguridad <sup>10</sup>

---

<sup>9</sup> Periódico La Nación digital <https://www.lanacion.com.ar/1912695-vigias-en-el-cielo-en-el-norte-habra-globos-aerostaticos-contral-narcotrafico> (Consulta 31 Enero 2019)

<sup>10</sup> Biblioteca Digital Chile <https://bibliotecadigital.indh.cl/handle/123456789/858>

#### *2.3.4. Del dron*

EL VANT, más conocido como “dron”, se usa en diferentes sectores: vigilancia de eventos, búsqueda de personas en situaciones de emergencia, vigilancias fronterizas, investigaciones arqueológicas, vigilancias medioambientales (incendios, delitos contra la ordenación del territorio, afectaciones de caminos públicos), para uso militar, y desgraciadamente para terrorismo (ejemplo de ello tenemos el presunto intento de asesinato a Nicolás Maduro en agosto de 2018, al parecer acontecido desde un dron) <sup>11</sup>

Son extremadamente funcionales, accesibles y veloces, por ello se vienen utilizando para todas estas cuestiones.

#### *2.3.5. Del radar*

Si bien los radares se desarrollaron inicialmente para un uso militar, hoy en día los podemos encontrar en diversidad de utilidades civiles, como la gestión del tráfico rodado, del tráfico aéreo, el conocimiento de la tierra y el agua (aplicación en geología, hidrografía, oceanografía y cartografía, entre otras), medición de la climatología y en medición de velocidad y ángulos. En cuanto a los sistemas de vigilancia, no podemos obviar que, dada la capacidad del radar para detectar objetos en la oscuridad o en condiciones de niebla, pueden ser aplicados como base para un detector de movimiento, lo cual se usa además para la vigilancia del tráfico (radar de control velocidad DGT y Ayuntamientos).

#### *2.3.6. Del satélite*

Además de los usos descritos en el apartado anterior como la predicción climática, televisión y comunicaciones, científicos, de defensa militar y para la navegación, en cuestiones de vigilancia de objetivos, algunos estados se sirven de ellos para el espionaje, sobre todo militar, para detectar bases de maniobras y escondites de armamento y para vigilancia de fronteras y contra el narcotráfico. De esto último a través, por ejemplo, del monitoreo de cultivos, detectando plantaciones de marihuana.

---

<sup>11</sup> El País Internacional

[https://elpais.com/internacional/2018/08/05/actualidad/1533422659\\_307629.html](https://elpais.com/internacional/2018/08/05/actualidad/1533422659_307629.html) ( consulta 31 Enero 2019)

## 2.4. Marco normativo

Cada vez estamos más controlados por los gobiernos. Nos están observando, y lo hacen a través de tecnologías de vigilancia como las expuestas en este epígrafe.

Analizaré en primer lugar las cámaras de vigilancia, pues sabemos que podemos encontrarlas actualmente tanto en establecimientos como en lugares públicos, para lo que se establecen normativas concretas en nuestro país:

Por un lado, es la **ley Orgánica 4/2015 de 30 de marzo** de Seguridad Ciudadana, la que en su artículo 22 establece que *“la autoridad gubernativa y, en su caso las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas lugares u objetos mediante cámaras de video vigilancia fijas o móviles legalmente autorizadas de acuerdo con la legislación vigente en la materia”*. Es por ello que estamos acostumbrándonos a ver cámaras en múltiples zonas de las ciudades. ¿Cuáles serán las *“cámaras fijas o móviles legalmente autorizadas”* a las que se refiere el artículo anterior?, pues bien para proteger a los ciudadanos y a los bienes en los espacios públicos, las Fuerzas y Cuerpos de Seguridad pueden emplear los medios técnicos oportunos a su alcance utilizándolos siempre bajo los principios de intervención mínima y proporcionalidad siendo los órganos administrativos que se determinen reglamentariamente los que puedan autorizar dichas instalaciones que será fijas cuando con ellas, y actuando siempre bajo los principios anteriormente mencionados, se pretenda asegurar la protección de particulares y bienes públicos así como cuando se pretenda prevenir y sancionar infracciones a la seguridad ciudadana <sup>12</sup>, y serán móviles cuando con ellas se pretendan apoyar las funciones previstas para las cámaras fijas y en aquellos casos en los que por extrema urgencia no puedan cumplirse los plazos de trámites previstos para la autorización por las autoridades administrativas y siempre que se cumplan los requisitos de idoneidad, proporcionalidad y que no se utilicen para la grabación de imágenes o sonidos del interior de las viviendas, siempre que, para este caso, no medie resolución judicial o autorización expresa del titular <sup>13</sup>

En esta misma normativa, se establecen los derechos de los interesados y el procedimiento de destrucción de grabaciones (imagen y sonido), así como el régimen sancionador del que incumpliera estos requisitos.

---

<sup>12</sup> Artículo 3 Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

<sup>13</sup> Artículos 5 y 6 Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Debemos tener en cuenta que la **Constitución Española de 6 de diciembre de 1978**, en su artículo 104 establece que *“Las Fuerzas y Cuerpos de Seguridad tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana. Una ley Orgánica<sup>14</sup> determinará las funciones principios básicos de actuación y estatutos de las Fuerzas y Cuerpos de seguridad”*. Queda establecido de esta forma el respeto absoluto a la Constitución y leyes con el que estos cuerpos deben actuar, velando siempre por la protección de personas bienes y libertades.

También se determina en la Constitución el derecho a la imagen (art.18.1CE) el cual determinará la información referida a rasgos físicos personales que pueden ser objeto de conocimiento o difusión por parte de terceros. *“Este bien jurídico se salvaguarda reconociendo a la persona la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de toda persona”* (SSTC 83/2002, de 22 de abril y 7/2007, de 16 de abril)<sup>15</sup>

En cuanto a la instalación de cámaras en empresas, se regirá por lo previsto en la **Ley de Seguridad Privada 5/2014** que dedica a este efecto su artículo 42 en el que regula este servicio prohibiendo en cualquier caso que puedan tomarse imágenes de los espacios públicos *“salvo en los supuestos y en los términos y condiciones previstos en su norma específica previa autorización administrativa por el órgano competente en cada caso”*<sup>16</sup> lo cual supone una gran novedad, puesto que este tipo de grabaciones eran, hasta ahora, exclusivas de las Fuerzas de públicas.

En estos establecimientos, las cámaras de vigilancia podrán ser instaladas en las zonas del comercio que estén abiertas al público, en los almacenes, salas del personal, lugares de cobro, pero nunca dentro de los baños o vestuarios. Tampoco podrán estar orientadas hacia el exterior (salvo que fuera estrictamente necesario).

Así, queda determinada la existencia de diferentes clases de video-vigilancia: la que, a través de una empresa de Seguridad Privada, se contrate por un empresario para

---

<sup>14</sup> Ley Orgánica 2/1986 de 13 de marzo de Fuerzas y Cuerpos de seguridad.

<sup>15</sup> ETXEBERRIA GURIDI, José Francisco y ORDENANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726. Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch, Valencia, 2010, pág.34-35.

<sup>16</sup> artículo 42.2 Ley 5/2014 de seguridad Privada

establecer la vigilancia en el centro de trabajo, y otra utilizada por las Fuerzas y Cuerpo de Seguridad en lugares públicos <sup>17</sup>.

¿De qué forma deben estar instaladas las cámaras en los establecimientos? Para ello, la **Ley Orgánica de Protección de Datos (LOPD)** <sup>18</sup> y el **Reglamento General de Protección de Datos (RGPD)** <sup>19</sup> europeo para los sistemas de video-vigilancia prevén la existencia de un fichero en el Registro General de Protección de Datos en el que tendrán que especificar cuál es la finalidad para la que se están grabando las imágenes. Además, los establecimientos habrán de informar sobre la existencia de video cámaras de manera expresa, precisa e inequívoca bebiendo contar con al menos un cartel informativo ubicado en lugar visible.



*Figura 8: cartel de video-vigilancia* <sup>20</sup>

Además de todo lo expuesto hay que añadir que la ley orgánica de protección de datos de carácter personal se aplicará como norma general cuando exista grabación, captación, transmisión, conservación o almacenamiento de imágenes o cuando dichas

<sup>17</sup> ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726. Ámbito de aplicación y derechos fundamentales afectados, Editorial Tirant lo Blanch, Valencia, 2010, pág. 46-47.

<sup>18</sup> Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

<sup>19</sup> RGPD 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016

<sup>20</sup> La AEPD actualiza el cartel de información de [videovigilancia](https://www.josemanuel sanz.es/la-aepd-actualiza-el-cartel-de-informacion-de-vidovigilancia/) <https://www.josemanuel sanz.es/la-aepd-actualiza-el-cartel-de-informacion-de-vidovigilancia/> publicado el 03/06/2018

actividades se refieran a personas identificadas o identificables. Esta ley de protección de datos, en principio, no será de aplicación en el ámbito personal o doméstico, puesto que cuando se contratan servicios de vigilancia privada en los domicilios, se entiende el consentimiento al establecerse la instalación de cámaras.

En cuanto a las vigilancias que se realizan con drones, la normativa exige que para sus pilotajes deban de cumplirse una serie de requisitos teóricos y prácticos, y que se obtenga una acreditación como piloto. Ésta acreditación no supone la mera licencia para poder operar por el espacio aéreo libremente, sino que deben de solicitarse las autorizaciones pertinentes para realizar los sobre-vuelos, así como informar la empresa, particular o Administración que lo requiera.

Será la Agencia Estatal de Seguridad Aérea (AESA) la encargada de la regulación del marco normativo completo del sector.

Es tal la importancia que están adquiriendo estos dispositivos tanto en labores de seguridad pública como privada, que nos encontramos ante cambios constantes de regulación legal.

Es un hecho probado que este tipo de aparatos se utiliza también en vigilancias gubernamentales y militarizadas.

De los radar y satélites debemos diferenciar el uso civil del militar, y mencionar que si bien no existe una normativa directa, se estará a lo dispuesto en los “*Tratados y principios de las Naciones Unidas sobre el espacio ultra-terrestre*”<sup>21</sup>, documento en el que se observa los tratados, convenios, acuerdos, declaraciones y demás principios que deben regirse en el espacio exterior. Este es un tratado de referencia, en el que se resumen los anteriores tratados del espacio que han sido aprobados por Naciones Unidas.

---

<sup>21</sup>PUBLICACIÓN DE LAS NACIONES UNIDAS.  
<http://www.unoosa.org/pdf/publications/STSPACE11S.pdf>

## 3. TECNOLOGÍAS DE SEGUIMIENTO

### 3.1. Aproximación al concepto

Podrían definirse como aquellas que consiguen generar un recorrido, las que nos permiten conocer dónde se encuentra una persona o un objeto sin necesidad de verlo. Nos indican el trayecto.

Un concepto que podemos relacionar en este apartado es la trazabilidad, entendida como el procedimiento que nos permite conocer la ubicación a través del rastreo.

En concordancia con lo anterior, existen una serie de dispositivos que permiten que seamos detectados, que puedan ser conocidos nuestros movimientos y zonas que hayamos visitado y, en otros casos, que podamos ubicar nuestros vehículos o cualquier objeto de interés al que hayamos dotado de alguno de estos utensilios.

El seguimiento que se realiza es en realidad un seguimiento del dispositivo que llevamos con nosotros.

### 3.2. Clasificación

#### 3.2.1.-Smartphones y Apps

Los *smartphones* se definen como teléfonos inteligentes, capaces de realizar funciones similares a las de una computadora, de manera inalámbrica. Permiten enviar archivos, comunicación directa audio-video, emiten señales que permiten su ubicación al estar dotados de GPS <sup>22</sup> y GSM <sup>23</sup> en el terminal, y también pueden ser localizados a través de las antenas de telefonía repartidas por todo el territorio nacional, y gracias a las tarjetas SIM <sup>24</sup> que transmiten señal.

Además, en los *smartphones* se pueden instalar diversas Apps, definidas como aplicaciones que combinan un programa con “gadget” de escritorio, cuyo funcionamiento puede o no, depender de internet. Se instalan para mejoras del rendimiento, para tener redes sociales, juegos, compras online, televisión online, música, gestores varios, mensajería...y un sin fin de posibilidades.

---

<sup>22</sup> Wikipedia, la enciclopedia libre: del Inglés “*Global Positioning System*” (GSM) <https://es.wikipedia.org/wiki/GPS> [consulta 11 febrero 2019]

<sup>23</sup> Wikipedia, la enciclopedia libre: Acrónimo GSM del inglés *Global System for Mobile communications* [https://es.wikipedia.org/wiki/Sistema\\_global\\_para\\_las\\_comunicaciones\\_móviles](https://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_móviles) [consulta 11 febrero 2019]

<sup>24</sup> Wikipedia, la enciclopedia libre SIM: acrónimo en inglés de *Subscriber Identity Module*, [https://es.wikipedia.org/wiki/Tarjeta\\_SIM](https://es.wikipedia.org/wiki/Tarjeta_SIM) [consulta 13 de Febrero]

Son de especial relevancia en este apartado las Apps relativas a geolocalización, puesto que con ellas será buscado un destino por el usuario, dejando al mismo tiempo el rastro de ese recorrido realizado al ser activada la aplicación. La mayoría de las Apps requieren tener activa la pestaña “localización” del dispositivo.

### 3.2.2. Tableta

Es un tipo de computadora sin teclado, donde el funcionamiento se da gracias al sistema táctil o multitáctil, que responde al tocar con los dedos la pantalla.

Se piensa que las tabletas harán desaparecer las computadoras, puesto que cada vez pueden llevar integrada mayor memoria y su facilidad de uso y transporte las hacen ser unos dispositivos de gran utilidad en el siglo actual.

Al ser similar a un *smartphone*, aunque de mayor tamaño, llevan integrados sistemas de localización como los definidos en el aparato anterior, haciendo posible que se puedan generar seguimientos del usuario del dispositivo.



Figura 9: Nube de iconos en un Smartphone <sup>25</sup>

Figura 10: Imagen Tableta. Fuente gadgetreview.com <sup>26</sup>

### 3.2.3. Wearables devices

Son dispositivos para llevar puestos, basados en tecnologías complejas que se controlan a través de un teléfono inteligente o computador. Han ido evolucionando con el paso de

<sup>25</sup> <https://mx.depositphotos.com/10062530/stock-photo-smartphone-with-cloud-of-application.html> [consulta 13 febrero 2019]

<sup>26</sup> <http://www.gadgetreview.com/reviews/tablet-reviews> [Consulta 13 febrero 2019]

los años desde los más usados smartwatches (relojes inteligentes) hasta pulseras de actividad (fitness wearables), chips para zapatillas deportivas (que transmiten la información de pasos y distancia a nuestros dispositivos *smartphones* o a nuestras computadoras) e incluso implantes intra-dérmicos (especialmente importantes en el control de algunas enfermedades en unos casos, y como localizadores de personas, en otros). Además, existen ya en el mercado *smartglasses* (gafas que ofrecen acceso a internet y a diversas aplicaciones, como la cámara) y *smartclothes* o ropas inteligentes que perciben temperatura corporal y control de funciones vitales.



Figura 11: Wearables devices (Fuente [imagenesmy.com](http://imagenesmy.com))<sup>27</sup>

#### 3.2.4. Big data

La capacidad de generar datos actualmente a nivel usuario es enorme. Cada vez más dispositivos están enviando datos constantemente desde sus sensores, siendo el Big Data esa cantidad de datos con tal volumen y complejidad que no pueden ser tratados por un software convencional. Su característica se define en torno a lo que se conoce como tres “V”, y que son el volumen de datos, la velocidad con la que estos se procesan y la variedad de fuentes de los que provienen.

También es necesario reflexionar sobre la veracidad de los datos obtenidos y el valor de estos, es decir qué relevancia tienen esos datos para cada uso concreto y así poder rentabilizarlos.

---

<sup>27</sup> <https://www.imagenesmy.com/imagenes/wearable-technology-definition-7e.html>

El *big data* obtiene los datos de diversas fuentes, incluyendo estructurados y no estructurados. Estos datos que se obtienen serán procesados, se les dará formato y se almacenarán cargándose de manera distribuida en varias fuentes, dividiendo así datos de gran tamaño en diferentes procesadores, con lo cual se logra mayor velocidad en la búsqueda y análisis de datos. Para abordar el análisis de tantos datos, el Big Data utiliza la lógica basada en algoritmos, empleando incluso varias ramas de la inteligencia emocional, como modelos predictivos y prescriptivos. Una vez hecho esto, se extrae el valor de los datos que se han analizado en forma de patrones de comportamiento, predicciones de compra, o identificaciones de oportunidad de negocio entre otras. Es un medio imprescindible para gobiernos y empresas por la gran capacidad de análisis de datos a ritmo de producción.

### 3.2.5. Redes sociales

Una red social es la unión de varias personas como nodos de comunicación que generan conexiones al compartir información. También se definen con un sentido más amplio como estructuras sociales conformadas por individuos que mantienen conexión por tener intereses comunes. Existen multitud de plataformas digitales que facilitan que las conexiones y la información que se genera entre las personas de una red social se expandan articulen y creen lazos de cooperación. Son estas plataformas del entorno digital desde donde nos movilizamos para compartir ideas e iniciativas.

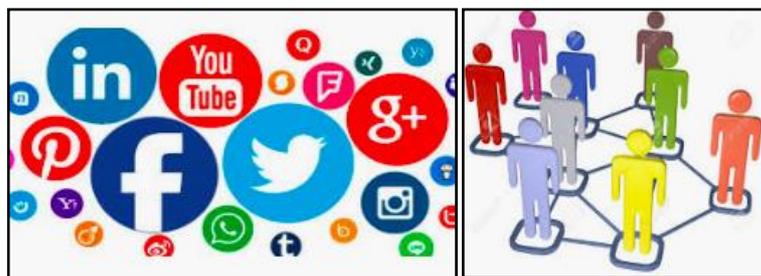


Figura 12: Nodos de comunicación y redes sociales <sup>28,29</sup>

<sup>28</sup> [https://es.123rf.com/photo\\_7794517\\_s%C3%ADmbolo-personas-conectan-en-los-nodos-de-la-red-de-medios-de-comunicaci3n-social-3d-.html](https://es.123rf.com/photo_7794517_s%C3%ADmbolo-personas-conectan-en-los-nodos-de-la-red-de-medios-de-comunicaci3n-social-3d-.html)

<sup>29</sup> <https://medium.com/@marvin.soto/el-fin-de-las-redes-sociales-como-las-conocemos-b6d6c041ac70>

Se utilizan también como canales de marketing, estableciendo relación con los usuarios para crear nuevas ventas. Con ellas se pueden mejorar servicios de atención al cliente gracias a la retroalimentación que se recibe (“me gusta”, “like”)

Las redes sociales han cambiado la forma de comunicación en el mundo, a través de internet, facilitando que podamos realizar un seguimiento tanto de otros individuos como de artículos en los que estemos interesados. Algunos ejemplos de redes sociales serán: Meetic, Spotify, youtube, Facebook.

### 3.2.6. Tecnología de seguimiento de usuarios de internet

Es de suma importancia que usemos internet de modo responsable. Debemos prestar atención en el tipo de información que compartimos, así como los sitios web que podemos visitar:

#### 3.2.6.1. Cookies y cookies flash

Las cookies no son archivos creados por un sitio web que contiene cantidades pequeñas de datos que se envían entre un servidor donde se aloja la página web y el navegador que estemos usando en ese momento. De esta forma se puede identificar la actividad de un usuario en un sitio web específico. Se obtiene un seguimiento de las preferencias web del usuario.

Cookie flash será definida como la “cookie” del usuario que visita un sitio web que utilice Adobe Flash. Su acrónimo del inglés es LSO <sup>30</sup>(*Local Shared Object*)

#### 3.2.6.2. Balizas Web

También conocidos como faros web <sup>31</sup> o web bug <sup>32</sup>, son archivos desarrollados para el seguimiento del usuario por web que pertenecen a una entidad determinada permitiendo a ésta la observación de cómo el usuario es capaz de navegar de una página a otra, haciendo con esta información que la navegación sea más sencilla y eficiente.

---

<sup>30</sup> [https://es.wikipedia.org/wiki/Local\\_Shared\\_Object](https://es.wikipedia.org/wiki/Local_Shared_Object) [en línea 23 febrero 2019]

<sup>31</sup> **faro web** por el término inglés *web beacon* [https://es.wikipedia.org/wiki/Web\\_bug](https://es.wikipedia.org/wiki/Web_bug) [en línea 23 febrero 2019]

<sup>32</sup> El término *web bug* proviene del inglés *bugging device*, es decir micrófono oculto<sup>4</sup> o "cucaracha" (*bug* significa “insecto”) [https://es.wikipedia.org/wiki/Web\\_bug](https://es.wikipedia.org/wiki/Web_bug) [en línea 23 febrero 2019]

La “uBeacon<sup>33</sup>”, o balizas de ultrasonido, son sonidos especialmente agudos no perceptibles al oído humano, y que emite el dispositivo que se está utilizando al visitar una página web que tenga instalada una baliza web. Esto permite al remitente averiguar qué dispositivos están conectados con otros ( por ejemplo, si tienes conectados el teléfono con el ordenador, etc.)

#### *3.2.6.3. Píxeles de seguimiento*

Conocidos como etiqueta pixel o como 1x1 pixel, no es más que un gráfico que se descarga cuando un usuario de internet visita un sitio web o cuando abre un correo. La utilidad del mismo es el monitoreo de acciones específicas del usuario. Se utiliza para obtener información, siendo su tamaño diminuto, por lo que no puede ser visto por el usuario. Se camuflan con el fondo de color del sitio web visitado. Recolectan información sin consentimiento del usuario, por lo que están siendo criticados en la actualidad. Son una alternativa a las cookies para los seguimientos de preferencias del navegante por la red.

#### *3.2.6.4. Browser Fingerprint Tracker*

Traducido al español como “localizador de huellas digitales del navegador”, constituyen otro método de monitorización o seguimiento del usuario, aunque éste haya bloqueado las cookies. Siempre que se realiza una visita de una página web, nuestro dispositivo informa a la página visitada de especificaciones acerca del sistema y ajustes del dispositivo que se está utilizando, es decir, con la visita de la página web, no sólo accedemos a información que estamos buscando, sino que la página se queda con una parte de nuestra “huella dactilar”. Se obtiene información a la vez que se transmite.

#### *3.2.6.5. Interfaces*

Definida como el medio a través del cual un usuario y un dispositivo pueden comunicarse. Es una conexión física entre sistemas que se compone de puntos de contacto entre el usuario y el equipo. Hace referencia al conjunto de elementos que aparece en la pantalla del dispositivo y que permiten que un usuario pueda realizar acciones concretas.

---

<sup>33</sup> Ultrasound Beacon <https://www.cookiebot.com>

### 3.2.7. Internet of things (IoT)

Define los objetos que usamos cada día y que se encuentran conectados a internet.

La base del *Internet of Things (IoT)* es precisamente la conectividad a la red. Consiste en dotar de componentes electrónicos a los aparatos, tanto para uso diario como para el uso industrial, diagnóstico a través de internet y uso administrativo, siendo muestra de esto las *Smart Cities* <sup>34</sup>. Este es un concepto que implica que TODO puede estar conectado y por ello controlado. También podemos definirlo como el proceso de interconexión de objetos permitiendo un intercambio automático de información con otros centros de control sin necesidad de intervención humana con resultado de obtención de información en tiempo real, de gran utilidad para las empresas y negocios.

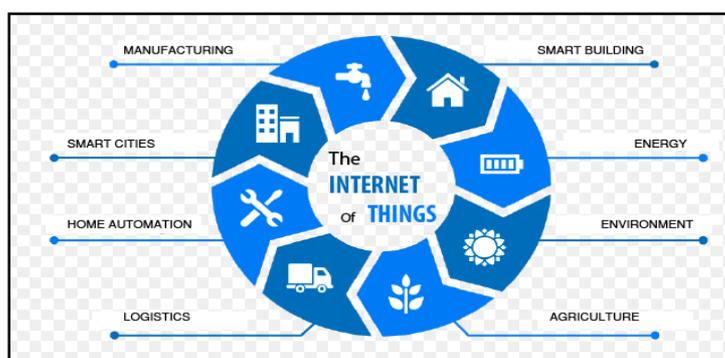


Figura 13: el Internet of Things<sup>35</sup>

### 3.2.8. Tecnologías de Información y Comunicación (TIC)

Son recursos, herramientas y programas que se usan para administrar, procesar y compartir información entre soportes tecnológicos.

Nos permite disponer de información inmaterial, puesto que se digitalizan archivos, reduciendo así los costes. La posibilidad de poder comunicarnos de forma instantánea las hace estar creciendo en el ámbito de las tecnologías modernas.

---

<sup>34</sup> BARRIO ANDRES, Moisés: «La smart city: version 2.0 del municipio», en *Documentación Administrativa: Nueva Época*, No 3, 2016.

<sup>35</sup> <http://www.starproperty.my/index.php/articles/property-news/what-is-the-internet-of-things/>



activos que forman una cadena de suministros, haciendo posible controlar en tiempo real el trayecto de los productos, así como el conocimiento de las mejores rutas para el transporte. El *big data* permite en éste ámbito recoger la información generada en los procesos para realizar las distribuciones, haciendo seguimientos de los productos y maquinarias.

Para los deportes, a través de una plataforma de seguimiento en tiempo real por medio de dispositivos que emiten señal GPRS (bien sea el propio *smartphone* o algún *Wearable device*) y por medio de una aplicación descargada previamente, los participantes pueden realizar la transmisión de datos, su velocidad, trayecto, recorrido y ésta ser recibida en tiempo real por quienes tengan acceso a esa aplicación. La empresa Valenciana *TraceMyWay* es pionera en desarrollo de ésta tecnología de seguimiento en tiempo real.

En cuestiones de sanidad y salud, dispositivos para el control de frecuencia cardíaca—bien sean colocados por cirugía, bien sean dispositivos externos como aplicaciones de ciertos Wearables, para los controles de ciertos niveles en sangre para algunas enfermedades. Es una garantía de vida el poder disponer de estas tecnologías en la actualidad. Mejoran la calidad de vida de los pacientes, que diariamente pueden tener su historial actualizado en su propio ordenador personal o dispositivo móvil.

A nivel de seguridad y justicia, se utilizan para controlar telemáticamente las medidas y penas de alejamiento

En ámbito laboral, como hemos visto en el apartado de las TIC, para el desarrollo profesional en cuanto a la realización de cursos de formación online (teleformación), así como para el fomento del tele-trabajo, que permite mejoras en conciliación laboral

En educación, este tipo de tecnologías permite un seguimiento específico y directo del trabajo en las que realizan los alumnos, pudiendo tener referencias claras y completas de los accesos a plataformas, de las repeticiones de ejercicios, de los errores cometidos...

En el ámbito policial, las tecnologías de seguimiento aportan datos relevantes a la hora de investigar y clarificar hechos delictivos, que- de otra forma- serían más difícil de solventar, tenemos como ejemplo el conocido caso de Diana Quer, para cuya resolución fue fundamental la triangulación de posicionamiento de su teléfono móvil las horas previas a la desaparición, así como el acceso a los datos de sus últimas conversaciones.

### 3.4. Legislación

El seguimiento a través de internet afecta de una u otra forma a nuestras vidas. De todos es sabido que para darse de alta en cualquier red social tenemos que facilitar una serie de datos personales. Una vez realizamos ese alta, estamos aceptando las condiciones de contrato y privacidad que posibilitan a las empresas a utilizar esos datos que hemos aportado.

El acceso a las redes sociales es relativamente sencillo. Los menores de edad, en concreto, los menores de 14 años no pueden acceder a las redes sociales, o mejor dicho no deben, pero sabemos que en ocasiones suelen hacerlo. Las normas más importantes que afectan a la protección de los menores y de los ciudadanos en general y en la red son:

- **Ley de Protección de Datos** que requiere que para publicar cualquier tipo de dato, información o archivo de personas, se requiera el consentimiento expreso y escrito de las mismas, pudiendo éste ser revocado en cualquier momento y en caso de menores de edad, en su artículo 13.1, el Reglamento de la Ley Orgánica de Protección de Datos exige que ambos progenitores presten consentimiento.

- **Reglamento Europeo de Protección de Datos 2016/679**, que otorga una protección específica al menor de edad en su artículo 38: *“Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.”* y que reconoce como un derecho fundamental del individuo el tratamiento de sus datos personales.

- **Ley de Propiedad Intelectual** puesto que la descarga libre y gratuita de contenidos que tengan derechos de autor es ilegal. La norma en vigor persigue especialmente a las páginas que ponen estos contenidos a disposición de otros usuarios y que buscan obtener beneficio de ello. En concordancia con lo mencionado, es importante tener en cuenta

Suele darse también en este tipo de plataformas el “usurpar una identidad”, lo cual es relativamente habitual en las redes sociales (tenemos casos de menores que suplantan

la identidad de sus padres para crear acceso a algunas páginas y/o redes) y casos en los que se utilizan imágenes de personas que encontramos por internet, y son utilizadas como si fueran la imagen de la persona que crea el perfil. Esto se conoce como se conoce como “*Phishing*”<sup>36</sup>

Usurpar la identidad de otros es considerado delito, pese a que no existe una regulación específica como delito de la suplantación de identidad, sino que el Código Penal regula cada caso de forma diferente en función de la acción que se haya llevado a cabo por el delincuente.

En el caso en que se cree un perfil en una red social y se utilice una fotografía de otra persona sin su consentimiento, estaremos ante un delito de vulneración a la propia imagen.

En el caso en que una persona entre en un perfil ajeno y robe contraseñas comete un delito de descubrimiento y revelación de secretos, lo que se llama “*hacking*”.<sup>37</sup>

Además, internet y sus redes sociales son plataforma ideal para la comisión de otros tipos delictivos como amenazas, estafa, injurias etc. sin olvidar la proliferación de delitos de “acoso” a través de redes.

En cuanto al IoT, que es donde destacan los dispositivos wearables, así como dispositivos de domótica controlados por internet, plantean serias dudas acerca de la protección de datos de sus usuarios, así como de la circulación de los mismos a través del mundo virtual. Hay que destacar el ya mencionado **Reglamento (UE) 2016/679 del Parlamento Europeo**, que permite a los ciudadanos el mejor control de sus datos, y observar la **Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016**, “*relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos*”, que se destinarán a ámbitos policiales y de Justicia.

En el ámbito laboral, no existe en la actualidad una normativa que regule completamente los cambios tecnológicos y los usos y reglamentaciones sobre las tecnologías de seguimiento que vienen utilizándose a menudo para el “control” del

---

<sup>36</sup> Término que proviene del inglés *fish* (pescar) y que fue adoptado por crackers que querían apropiarse de cuentas de víctimas anónimas

<sup>37</sup> Refiere al intrusismo informático

trabajador, pudiéndose vulnerar alguno de sus derechos individuales (se controlan horarios de entrada y salida, descansos en la jornada, trayectorias seguidas.), con fines de incrementar la productividad laboral, y por ende, la economía del empresario.

## 4. TECNOLOGÍAS DE LOCALIZACIÓN

### 4.1. Aproximación al concepto

Aquellas que nos permiten ubicar cualquier objeto en un lugar determinado. Las personas pueden ser localizadas siempre que sean portadoras de dispositivos que estén dotados de este tipo de tecnologías.

### 4.2. Clasificación

#### 4.2.1. *Sistemas de posicionamiento por satélite*

Son los sistemas compuestos por diversos satélites que emiten y transmiten rangos de señal que hacen que se pueda establecer la localización y posicionamiento del receptor en cualquier parte del mundo. Proporcionan información muy exacta.

##### 4.2.1.1. *GPS*

*Global Positioning System* es un sistema de localización o navegación creado en 1973 por el Ministerio de Defensa de EEUU y con aplicaciones exclusivas de uso militar en un primer momento, que funciona a base de satélites y que sirven para localizar personas, y objetos o para viajar siguiendo rutas descritas...Triangulan la información en base a la latitud, altitud y longitud.

Los primeros en usar este tipo de tecnología fueron los militares, y actualmente lo utilizamos para navegación, en telefonía y para localizaciones con un margen de error mínimo y en tiempo real.

¿Cómo es su funcionamiento? El satélite manda un mensaje con la hora y así es calculada la distancia hasta el satélite. Dado que estas ondas viajan a la velocidad de la luz, podemos calcular la distancia una vez conocemos los minutos que se ha tardado en recibir el mensaje que emitió el satélite. Cuando conocemos la distancia hasta el satélite, sabemos que estamos en la superficie de una esfera imaginaria centrada en el satélite. Con dos satélites, estaremos en la intersección de ambas esferas. Con tres satélites reducimos las probabilidades a dos puntos y con cuatro resolvemos la ecuación y obtenemos precisión. Tenemos así las tres dimensiones longitud, altitud y latitud, junto con el tiempo cuadrangulando de esta forma, mejorando la posición con respecto a la triangulación.

En GPS se utilizan 24 satélites, 4 satélites en 6 órbitas MEO de altura media 20.000 Km inclinados 55°. Por ello la precisión de esta tecnología es de alta fiabilidad con error de pocos metros.

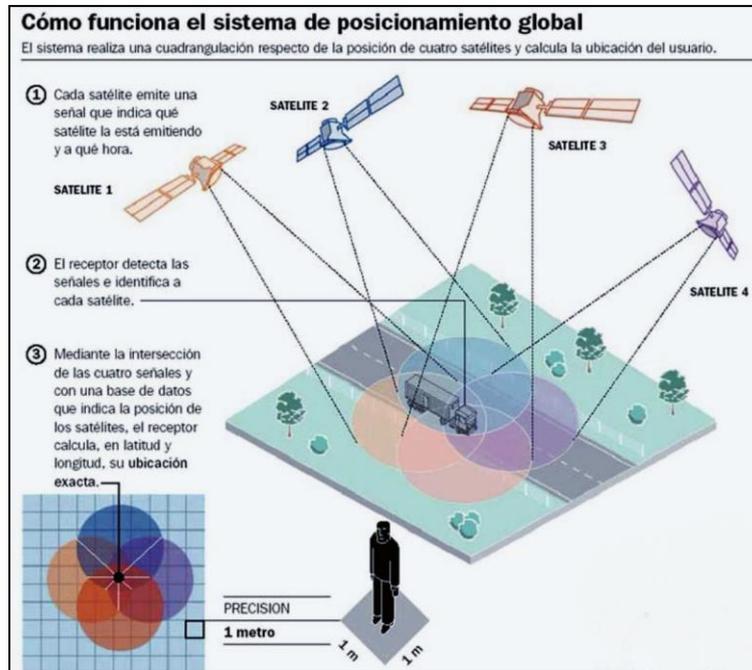


Figura 15: Sistema de Posicionamiento Global<sup>38</sup>

#### 4.2.1.2. GLONASS

*Globalnaya Navigatsionnaya Sputnikovaya Sistema* es el sistema de posicionamiento global creado por la Unión Soviética, de funcionamiento similar al del GPS, aunque su funcionamiento depende de 31 satélites que giran alrededor de la tierra, permaneciendo activos siempre 24 de ellos. Funciona igualmente por cuadrangulación por lo que necesita 4 satélites a la vez para obtener la correcta posición. Pese a que fuera iniciado su desarrollo en el año 1976, no fue hasta 1993 cuando entró en funcionamiento. Actualmente opera a nivel mundial sin restricciones, y en la mayoría de dispositivos “wearables”, por lo que localizar a sus portadores es meramente factible.

<sup>38</sup>Fuente:<https://www.facebook.com/tecnosim/photos/a.1832781376981757/1842717479321480/?type=1&theater>

#### 4.2.1.3. Galileo

Sistema de posicionamiento europeo, desarrollado por la Unión Europea y por la Agencia Espacial Europea, dotando así a este continente de tecnología independiente a las ya creadas por la Unión Soviética y los Estados Unidos.

Actualmente cuenta con 26 satélites en el espacio, y nos ha dotado de precisión de hasta 1 metro, y con una muy estable red. Este sistema ofrece tres tipos de servicio basados en la navegación por satélite:<sup>39</sup>

Uno para consulta de posicionamiento gratuita, constituyendo un servicio más fiable y exacto en relación con otros sistemas de localización. Como ejemplo práctico de su utilización, mencionar que Galileo permite que el sistema obligatorio de vehículos eCall (Sistema de emergencias obligatorio en vehículos europeos desde abril de 2018) pueda comunicar a los servicios de emergencia cual es la posición real del mismo. (Esto supone un gran avance para la localización de emergencias de tráfico.)

Galileo también posee un servicio de búsqueda y salvamento que se realiza desde la emisión de una señal de socorro mediante baliza compatible, haciendo posible la detección de la persona en tiempo reducido.

Otro de los servicios que presta es el “PRS”, o “servicio público regulado”, destinado a cuestiones de seguridad, militares y de administraciones en entorno encriptado y perfectamente seguro, manteniendo la continuidad del servicio incluso en condiciones adversas.



*Figura 16: Cuadrangulación de satélites* <sup>40</sup>

<sup>39</sup> [abogacia.es](http://abogacia.es) artículo de “Actualidad Delegación” publicado el 31 de agosto de 2018

<sup>40</sup> Fuente: European Space Agency

#### 4.2.1.4. Otros satélites a considerar

Es tal la competencia a nivel mundial sobre “Nuevas tecnologías”, que resulta importante, cuanto menos, mencionar la existencia de otros satélites que operan como alternativa a los anteriores. Serían:

Beidou- 2Tf: Es el sistema de posicionamiento global creado por el gigante asiático, en un principio para evitar la dependencia del GPS estadounidense, y que espera tener 35 satélites con 5 en órbita terrestre geoestacionaria (GEO) para 2020. Es conocido también como COMPASS. El nombre “Beidou” significa “Osa Mayor”.

IRNSS: Es el sistema de navegación satelital indio (*Indian Regional Navigation Satellite System*), cuyo objetivo principal para el que fue desarrollado fue la prestación de servicios de navegación, sincronización y posicionamiento preciso para sus usuarios. Cuenta con un servicio de posicionamiento estándar y uno restringido. Consta de satélites en órbita geoestacionaria (GEO) y en órbita geo síncrona (OSG)

GPS OCX: También conocido como GPS III, el OCX (*Next Generation Operational Control System*) es un sistema estadounidense que comandará todos los satélites GPS modernos, pues se trata de un método de control de operaciones de próxima generación. Proporcionará mayor seguridad cibernética al mismo tiempo que administrará señales civiles y militares de navegación. Este sistema mejoraría la cobertura y sería más preciso al estar dotado de tecnología anti-interferencias. Este tipo de satélites duran el doble que los actuales, pero no estarán operativos hasta la segunda mitad de 2021. Su auge viene determinado por los continuos avances tecnológicos a los que la sociedad se ve inmersa.

#### 4.2.2. Geolocalización

Es una herramienta por la que se obtiene la localización geográfica real de cualquier objeto o persona que porte un dispositivo conectado a internet o un GPS. Usado con fines militares en un primer momento, actualmente la geo localización es muy fiable a través de satélite (debiendo, al menos, de ser visibles al dispositivo 4 de ellos para determinar los parámetros de altitud, latitud, longitud).

Existen varios tipos de geo localización:

- La georreferenciación, o localización física.
- La geo codificación, o proceso para asignar coordenadas a un lugar.

- El geo etiquetado, proceso por el que podemos referenciar la ubicación de alguna fotografía que nos interese.

Con la geo localización, se han obtenido grandes avances en logística, en innovación tecnológica de automóviles, en rastreos de investigaciones policiales e incluso en ámbitos de justicia con la asignación de pulseras de localización a presos.

En el ámbito privado, el usuario de, por ejemplo, un teléfono móvil puede localizar un restaurante con facilidad, y cuando se utilizan las redes sociales puede compartir su ubicación con amigos y otros usuarios. Aplicaciones como Google Earth o Maps son claros ejemplos del uso de la geolocalización.



*Figura 17: Representación gráfica de Geo localización<sup>41</sup>*

#### *4.2.3. Localización GSM*

El rastreo de un teléfono móvil y la localización del mismo era, hace algunos años una empresa reservada para organizaciones militares, policiales y gubernamentales.

Este es el método más utilizado para localizaciones de personas desaparecidas en investigaciones policiales. La ubicación se obtiene gracias a la forma en que se comunica el terminal con la red de telefonía en general.

La localización GSM consiste básicamente en la realización de una triangulación de señal recibida de antena de red de telefonía. Las empresas operadoras de telefonía móvil

---

<sup>41</sup> Fuente: <https://www.lowi.es/blog/como-desactivar-la-geolocalizacion/>

ofrecen servicios GSM que permiten determinar la posición del terminal mediante la aproximación de las torres de telefonía, por la fuerza de la señal recibida y por el tiempo en que la señal tarda en transmitirse de una torre a otra. La localización se produce gracias a la triangulación de señales de radio entre varias torres de red de telefonía, y el terminal telefónico en sí.

Si se utilizara el terminal móvil con GPS, la localización, por motivos obvios ya analizados y al usarse conexión satelital, mejoraría notablemente la precisión de la localización.



Figura 18: Localización por radio-frecuencia telefonía móvil<sup>42</sup>

#### 4.2.4. Tecnologías de localización LBS y Localización en Tiempo Real (RTLS)

La Localización Basada en Servicios (LBS), también conocida como Localización Dependiente de Servicios de Información (LDIS) hacen referencia a cómo proveer servicios geográficos en tiempo real. Buscan la oferta de un servicio personalizado, utilizando para ello Sistemas de Información Geográfica junto a tecnología de comunicación de redes y tecnología de posicionamiento. Gracias a la geo localización y a la conexión a internet, las empresas que utilizan este tipo de tecnología pueden detectar la ubicación en la que se encuentran los usuarios consumidores y ofertar servicios determinados. Así las empresas mejoran su imagen y alcance ante el usuario.

Los RTLS (*Real Time Location System*) son sistemas utilizados para localizar objetos o personas en tiempo real. Funcionan por transmisión de señal a través de puntos de referencia que serán transmisores y receptores de esta señal.

---

<sup>42</sup> Fuente: Periódico La Razón

Observaremos ahora diferentes tecnologías de localización LBS y RTLS:

#### 4.2.4.1. *Visible Light Communication (VLC)*

También conocida como LiFi (*Light Fidelity*), constituye un tipo de conexión a internet. Es una tecnología novedosa, ecológica, económica y segura puesto que trasmite datos a través de la luz LED, por lo cual es indicado para lugares que son sensibles a emisiones electromagnéticas, al ser una tecnología que no utiliza la radiofrecuencia.

La luz LED transmite los datos de forma inalámbrica, sirviéndose para ello de luz que sea visible, o bien ultravioleta o infrarroja. Por ello, este sistema asegura la velocidad y la seguridad (no se conocen efectos nocivos de la luz en su incidencia sobre las personas).

Se estima que este método de conexión será la solución a los problemas que se plantean con tecnologías que se sirvan del ancho de banda.



Figura 19: Funcionamiento LiFi. Fuente [andinalink.com](http://andinalink.com)

Como desventaja principal, esta tecnología, al no atravesar paredes, precisa de mayor número de aparatos emisores, aunque por esto mismo, aumenta la seguridad al no expandirse los datos fuera de la habitación donde se esté utilizando.

#### 4.2.4.2. *Sensores inerciales*

También llamados IMU (Unidad de Medición Inercial), se configuran cómo sensores mediante los que, toda vez instalados o integrados en un dispositivo, se obtienen referencias de velocidad, orientación y posición del objeto determinado.

Estos resultados vienen dados por la disposición en este sensor de un acelerómetro (que determina los cambios de velocidad y la aceleración), un giroscopio (que nos indicará la dirección) y un magnetómetro (que funciona como una brújula, señalando el norte magnético)

Su principal finalidad estriba en la transmisión de datos de posición y/o desplazamiento, utilizándose principalmente para robótica, medicina, deportes (biomecánica del movimiento), realidad virtual, aviación...

#### 4.2.4.3. *Ultrasonido*

Son ondas sonoras de alta frecuencia (superior a 20.000 hertzios), por lo que no son perceptibles al oído humano, aunque sí lo sean para algunos animales como los delfines o los murciélagos.

Esta tecnología funciona cuando el sonido se dirige hacia un cuerpo a través de un traductor. Las ondas rebotan y se produce un “eco de onda” que es recibido por un ordenador o dispositivo apropiado reflejando así una imagen.

Los ultrasonidos tienen múltiples aplicaciones en la actualidad, sobre todo en medicina, permitiendo, entre otras, localizar exactamente la ubicación de quistes, mediante la ecografía (al proyectarse la onda, ese patrón se digitaliza y así se logra la imagen), para localizar materiales y daños en el interior de los mismos, etc.

Es una tecnología especialmente útil en Policía científica y forense puesto que se han podido localizar restos óseos humanos a través de ultrasonidos de alta frecuencia. Además, con ella se pueden realizar intervenciones en caso de graves catástrofes como pudiera ser el derrumbe de un edificio, para establecer daños y localizar seres vivos.

#### 4.2.4.4. *Bluetooth Low Energy (BLE)*

Se trata de una tecnología de transmisión de datos que usa de redes inalámbricas de uso personal WPAN para transmitir datos (imágenes, música) o voz. Esta transmisión se realiza por radiofrecuencia. Este tipo de *Bluetooth LE (Low Energy)* proporciona un mínimo consumo de energía, minimizando así los costes de mantenimiento del producto. Permite vinculación con otros dispositivos como tabletas, *smartphones* y computadores. Son localizables a través de aplicaciones que muestran la intensidad de la señal siempre que permanezcan conectados, y también al estar vinculados a otros dispositivos tecnológicos que mantengan conexión de red o wifi.

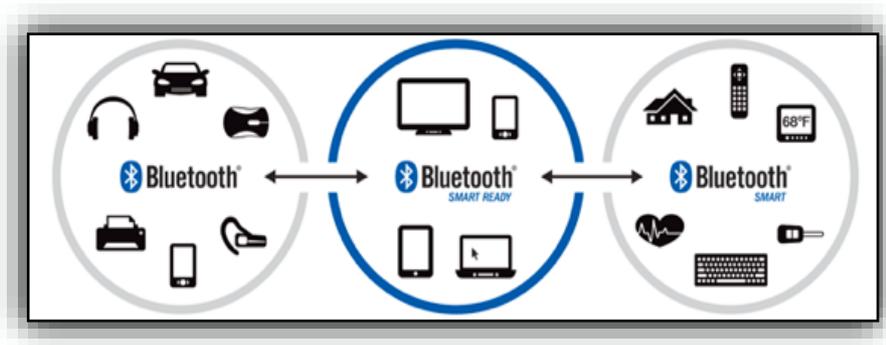


Figura 20: Aplicaciones del BLE. Fuente: <https://blogs.deusto.es>

#### 4.2.4.5. Wi-Fi

Es sin duda la tecnología de comunicación inalámbrica más conocida a nivel mundial. A través de ella, podemos conectar a internet multitud de equipos electrónicos, que se sirven de radiofrecuencia o infrarrojos para transmitir la información.

Lo usamos constantemente para vincular equipos entre sí. El referente de la comunicación sin cables.

Su funcionamiento se establece a partir de un enrutador (dispositivo conectado a internet por cable y que posee una antena) que distribuye la señal de manera inalámbrica dentro de un radio determinado. Existen equipos receptores que se encuentran dentro del radio de acción de la cobertura que emite la antena. En este sistema, la proximidad es fundamental, es decir, mientras más cerca se esté de la antena, mejor será la calidad de la señal, y con ello la conexión.

¿Podemos ser localizados por WiFi? En realidad, sí. Aún sin tecnología GPS o con la misma desconectada, el hecho de que nos conectemos a una red WiFi permite que seamos localizados. Esto es posible por la “localización MAC” de dicha señal: Nuestro dispositivo recibe la señal wifi a la cual nos conectamos, pero también recibe señales de wifi próximas a nuestra ubicación. Por ello, es posible que se realice una triangulación de las direcciones MAC de la zona donde nos encontramos, permitiendo así nuestra localización.

#### 4.2.4.6. Ultrawideband (UWB)

Tecnología que fue desarrollada por la década de los 60 para usos principalmente militares y gubernamentales cuyo funcionamiento consiste en la transmisión de impulsos de energía de muy corta duración proporcionando por ello un espectro de

frecuencias de varios giga hertzios de ancho de banda. Esta tecnología es capaz de transmitir sonido, imágenes y datos digitales en general. Si lo comparamos con otras tecnologías, como el WLAN o el UWB, proporciona una alta eficiencia de potencia con pocas interferencias de señal, aunque con alcance limitado, lo cual supone una gran desventaja.

#### 4.2.4.7. Radio Frequency Identification (RFID)

Este tipo de tecnología funciona identificando a través de radiofrecuencia, mediante un lector y sin que medie contacto. Para ello, es necesario que exista una etiqueta (tag) que esté adherida a un artículo determinado que queramos identificar, o que sea portada por una persona, o instalada en algún producto de un establecimiento, por ejemplo.

El funcionamiento es muy simple: el lector realiza por radiofrecuencia una serie de “cuestiones” al chip integrado en las tags RFID, que emitirán una señal de respuesta permitiendo que el objeto que lleva esa etiqueta sea identificado en tiempo real de forma precisa. Los códigos que se emplean en estas identificaciones del lector son códigos equivalentes a huellas dactilares, es decir, códigos únicos y personalizados. Este sistema usa de bandas de frecuencia de diferente rango (baja frecuencia, alta frecuencia, ultra alta frecuencia y microondas) que hacen variar el rango de distancia a la que se puede encontrar el objeto con etiqueta RFID.

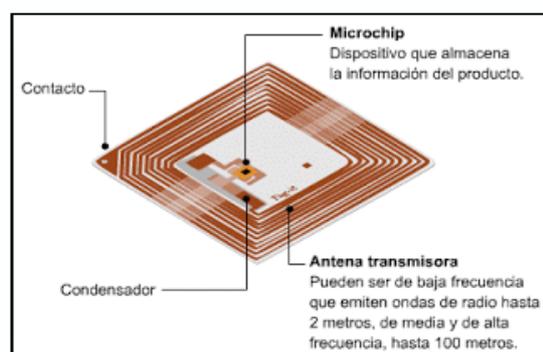


Figura 21: Etiqueta RFID<sup>43</sup>

Hay que señalar, además, que existes tres tipos fundamentales de etiquetas RFID:

Tags pasivos (no precisan alimentación interna), tags semi-pasivos (poseen fuente de alimentación propia para alimentar al microchip interno, pero no para transmitir señal) tags activos (usan la alimentación de una batería, pudiendo emitir señal y ampliando la cantidad de datos a procesar).

<sup>43</sup> Fuente: <http://subarasi.com.mx/etiquetas-termicas/etiqueta-rfid.html>

Podemos encontrarlos por todas partes. En las etiquetas de ropa, como tarjetas llave, en productos del supermercado, el artículo de grandes almacenes para evitar hurtos. Es una tecnología habitual y muy presente en el día a día, utilizada para mantener los objetos ubicados y localizados.

#### 4.2.4.8. Zigbee

Constituyen protocolos de comunicación inalámbrica, que transmiten sobre redes malladas pequeñas cantidades de datos. Esto permite un gran ahorro de baterías de los dispositivos que usan de esta tecnología puesto que el consumo energético es bajo. Por ello pueden abaratare los costos de fabricación de éstos.

Al igual que el *bluetooth*, opera bajo norma IEE 802.15, aplicándose generalmente en el IoT. Su objetivo serán aplicaciones que requieran comunicaciones seguras (redes inalámbricas de área personal WLAN) y como principal ventaja se nos muestra ideal en conexiones punto a punto. Son útiles baratos de construcción sencilla, aunque con poca cobertura, por lo que podemos decir que una de sus desventajas será la baja transferencia de datos.

Se utilizará para controles industriales, recolección de datos médicos, detección de humos, sensores de presión sanguínea, micrófonos, altavoces, y timbres o botones de alerta ante emergencias, siendo esto último muy útil en caso de poder localizar la situación de emergencia.

Esta tecnología funciona muy bien en entornos rurales, donde las capacidades de otras conexiones están minimizadas precisamente por las características del terreno.



Figura 22: Zigbee. (Fuente: <https://www.ecured.cu/ZigBee#/media/File:Zigbee.jpg>)

### 4.3. Usos

Los sistemas de localización por satélite se utilizan en el ámbito civil para rastreos de vehículos, consultas de logística (transporte de mercaderías y caudales), para realizar determinadas actividades, como el senderismo, en emergencias (para ubicar el lugar, la posición del que precisa la atención), para meteorología, ciencia, oceanografía, aplicaciones geodésicas, en topografía y agricultura.

También existen usos militares (los “spy Satélites” para localizar armamentos y dirección de las tropas) gubernamentales y de defensa. Se utilizan para la navegación aérea (control del tráfico aéreo).

En cuanto a la geo localización, hemos comprobado que se trata de una tecnología muy utilizada en la actualidad. Hoy día existen muchos negocios y empresas que usan este sistema para publicitarse, o para vender productos (*geocommerce*), o para situarse en un mapa web y que los usuarios tengan acceso visual de ellos en sus dispositivos. A nivel privado, con la geo localización somos capaces de informar del lugar donde nos encontramos en tiempo real.

La localización GSM se utiliza principalmente para establecer la ubicación de un dispositivo móvil que lleve insertada una tarjeta SIM. Con este sistema, la Policía y la Guardia Civil, han podido resolver numerosos casos de desapariciones y de criminalidad gracias a la colaboración de las compañías telefónicas en lo referente a la información que se recibe en las antenas receptoras de señal.

Con la localización en tiempo real conocemos la ubicación en el momento. Podemos localizar un artículo o una persona en un momento determinado, y podemos situarlos en un lugar concreto. Esto permite a las Fuerzas de Seguridad obtener pruebas para aportar a sus investigaciones, lo cual hace años sólo podían quedar en meras suposiciones difíciles de comprobar.

Sistemas utilizados Por las Fuerzas de Seguridad Españolas:

SIVE <sup>44</sup> (Sistema Integrado de Vigilancia Exterior) de la Guardia Civil, que es un sistema combinado de vigilancia, seguimiento y localización con el que se detectan

---

<sup>44</sup> SIVE (Sistema Integrado de Vigilancia Exterior)  
<http://www.guardiacivil.es/es/prensa/especiales/sive>

embarcaciones a larga distancia, coordinando así el seguimiento de las mismas para su interceptación.

Este sistema está provisto de unas “estaciones sensoras” que detectan los objetivos, visualizados a través de cámaras de video y de infrarrojos, unas antenas para emitir las comunicaciones en tiempo real de voz y datos, y un centro de control para efectuar las órdenes correspondientes de interceptar las embarcaciones.

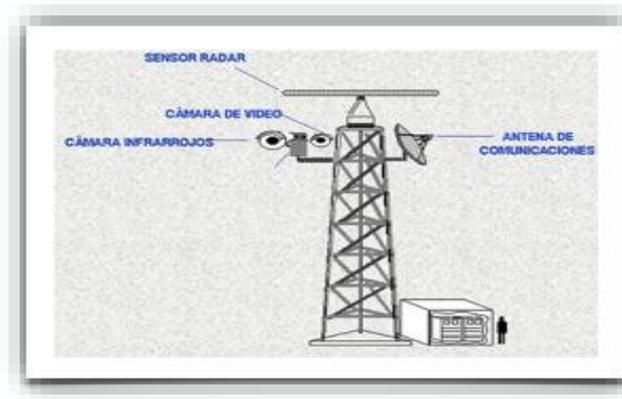


Figura 23: Capacidades del SIVE. Fuente: [guardiacivil.es](http://guardiacivil.es)

El proyecto PERSEUS <sup>45</sup> (Sistema Inteligente de Control de Fronteras) es también un sistema combinado que usa de todas estas tecnologías, cuyo objetivo es la vigilancia marítima en todo el territorio europeo, mediante el uso inteligente de la vigilancia.

ALERTCOPS <sup>46</sup>, es una aplicación móvil con la que podemos enviar nuestra ubicación a la comisaría o puesto de control más cercana a nuestra posición de modo discreto. Podemos chatear con la Policía, y denunciar la comisión de un delito que se esté produciendo. Con esta aplicación podemos usar el “modo guardián”, con el que podemos compartir nuestra posición con familiares que tengan instalada la aplicación. También se reciben alertas policiales en caso de emergencias próximas a nuestra ubicación.

---

<sup>45</sup> PERSEUS (Sistema Inteligente Control de Fronteras.) Ministerio del Interior. Guardia Civil <https://guardiacivil.es/>

<sup>46</sup> Ministerio del Interior. Dirección general de Policía <https://alertcops.ses.mir.es/mialertcops/>

#### 4.4. Legislación

Ya en el apartado anterior hemos visto como existen dispositivos que son utilizados por el sistema judicial para el control de presos. Pues bien, la posibilidad de localización que generan los mismos se debe a la tecnología GPS de la cual se les dota, y que hemos desarrollado en este epígrafe.

Con la **Ley Orgánica 5/2010 de 22 de junio** de reforma del Código Penal, se pone a disposición del Ordenamiento penal español las medidas tecnológicas de vigilancia penitenciaria vía satelital, con lo que se consigue una supervisión electrónica que permite atestiguar la presencia de un individuo en un lugar determinado. El sistema de vigilancia tendrá unas acotaciones que delimitan el espacio por el que el sujeto podrá circular, y especialmente a qué lugares no podrá acercarse.

Cuando hablamos de geo localización para el usuario medio, debemos tener presente el derecho fundamental de la intimidad y secreto de comunicaciones previsto en el artículo 18 de la **Constitución Española de 1978**, puesto que es un derecho que se ve afectado (tal como referimos en el apartado de tecnologías de vigilancia). Puede existir una vulneración de esta intimidad cuando somos geo localizados a través de nuestro terminal celular. El concepto de geo localización no está bien definido en nuestro sistema jurídico, por lo que es posible recurrir a **Directivas europeas como la 2002/58/CE de Privacidad**, que define en su artículo 2 la localización como *“Cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público”*. y en su artículo 9 apartado 1, dictamina el concepto de datos de localización distintos a los de tráfico: *“los relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico”*. Es decir, no se puede tener acceso a datos de localización sin consentimiento, siempre que no se trate de datos anónimos.

La policía Judicial atendiendo a casos de urgencia sí que tiene reconocida legitimidad para acceder a los datos de un terminal celular, tal como se deduce de sentencias del **Tribunal Supremo 316/200 de marzo y 1235/2002 de 27 de junio.**

## 5. CONCLUSIONES

En definitiva, hemos podido comprobar que el principal sistema de vigilancia que se utiliza en mayor medida y en cualquier ámbito es el sistema de video-vigilancia. Es el dispositivo más accesible pues nos permite tener imágenes y podemos utilizarlo casi de inmediato. No debemos olvidar que en nuestros teléfonos móviles llevamos incorporada cámara de video, y que todos en la actualidad la hemos utilizado alguna vez para tener un recuerdo, grabar un acto importante o gastar una broma. Podemos ver lo que ha ocurrido, y lo que está ocurriendo. Nos permite tener un medio de “prueba” en un momento determinado. Es un medio al alcance de todos que puede utilizarse bien por sí solo, bien instalado o implementado en otros dispositivos que se sirven de ellas para tener controladas diversas zonas como en globos, drones o antenas.

Hoy por hoy el uso de estos dispositivos está regulado en nuestro país. Es por ello por lo que las cámaras y video cámaras se deben de utilizar conforme a esa normativa, no pudiendo ser tenidas en cuenta las grabaciones de personas sin su consentimiento.

Son las Fuerzas de Seguridad, en su afán de garantizar la seguridad pública las que pueden usar videocámaras en su sentido amplio, siempre que dicho uso se fundamente de forma proporcional y aplicando el derecho de intervención mínima.

La privacidad es, en este caso, el bien jurídico que se ve más afectado. Es por ello que la Ley de Protección de Datos tiene una relevancia importantísima en los temas tratados en este trabajo. Por otro lado, las tecnologías de seguimiento han sido especialmente relacionadas con el concepto de acceso a datos personales, sobre todo a través de dispositivos móviles. Nuestros datos viajan y no parece que tengamos el control sobre ello.

Al producirse transmisión de información personal no es difícil conocer cuáles serán nuestros movimientos. Seremos predecibles en multitud de situaciones y no precisamente por ser vigilados, sino por proporcionar información propia de manera altruista.

La conexión a internet permite que se realice la localización de nuestros dispositivos, por lo tanto, en un elevado porcentaje se tiene conocimiento de nuestra ubicación, así como de nuestras rutinas.

Pese a ello, las tecnologías de localización y seguimiento son de gran utilidad en muchos campos, como por ejemplo en la protección de víctimas de delitos (en caso de

las víctimas de violencia de género se utilizan pulseras que ubican la posición de la persona denunciada para controlar las órdenes de alejamiento), y en caso de vigilancia penitenciaria se puede proporcionar medidas de reinserción social ajustadas a derecho puesto que ya se hace menos necesario que el ingreso en prisión sea permanente.

En la resolución de casos en investigación. Tenemos constancia de situaciones en las que se han podido esclarecer hechos gracias a las ubicaciones de telefonía móvil que han podido realizarse por los cuerpos de seguridad a veces para localizar desaparecidos y otras para realizar el patrón de movimiento de un presunto culpable de delito.

Se deduce así que con las nuevas tecnologías aplicadas al entorno de la criminología, se gana más de lo que nos parezca que se puede perder: por un lado, si bien nos cuesta parte de nuestra intimidad, de forma legitimada cuando somos grabados por cámaras de vigilancia en entornos públicos, se aumenta el canon de seguridad en dichos espacios.

Así es como debe de ser. Siempre que aprendamos a utilizar las nuevas tecnologías de forma eficaz, tendremos mucho que ganar. Debemos confiar en los poderes públicos y en nuestras Policías, y acatar las normas que regulan estas cuestiones.

## 6. REFERENCIAS BIBLIOGRÁFICAS

- ✦ BARRIO ANDRÉS, Moisés “*Internet de las Cosas*” Madrid, Editorial REUS S.A. 2018 [https://www.editorialreus.es/static/pdf/primeraspaginas\\_9788429020380\\_internetdelascosas.pdf](https://www.editorialreus.es/static/pdf/primeraspaginas_9788429020380_internetdelascosas.pdf) [En línea] [Consulta 24 febrero 2019].
- ✦ CASADO-MANSILLA Diego, LÓPEZ-DE-ARMENTIA Juan, Investigadores de DeustoTech Internet “*EL INTERNET DE LAS COSAS Y LA SOSTENIBILIDAD MEDIOAMBIENTAL*” 19 Enero 2015 <http://revistaingenieria.deusto.es/tag/iot/> [En línea] [Consulta 24 febrero 2019].
- ✦ ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726. Ámbito de aplicación y derechos fundamentales afectados, editorial Tirant lo blanch, Valencia, 2010.
- ✦ GUDIN RODRIGUEZ-MAGARIÑOS, Faustino. “Nuevos Delitos Informáticos: Phising, Pharming, Hacking y Cracking”, mayo 2008. **SP/DOCT/3705** <http://web.icam.es/bucket/Faustino%20Gud%C3%ADn%20-%20Nuevos%20delitos%20inform%C3%A1ticos.pdf> [en línea] [Consulta 11 de Marzo 2019].
- ✦ MINISTERIO DEL INTERIOR. GOBIERNO DE ESPAÑA. “*Guía sobre el uso de las cookies*” [en línea][consulta 04 de Marzo 2019] [http://www.interior.gob.es/documents/10180/13073/Guia\\_Cookies.pdf/7c72c988-1e55-42b5-acee-f7c46a319903](http://www.interior.gob.es/documents/10180/13073/Guia_Cookies.pdf/7c72c988-1e55-42b5-acee-f7c46a319903)
- ✦ PEREZ PORTO, Julián y MERINO María. Publicado: 2011. Actualizado: 2014. Definición de interfaz (<https://definicion.de/interfaz/>) [Consulta 24 febrero 2019].
- ✦ PONCE, Isabel *Monográfico: Redes Sociales*, Observatorio Tecnológico del Ministerio de Educación Cultura y Deporte. Gobierno de España, año 2012 [en línea] <http://recursostic.educacion.es/observatorio/web/en/internet/web-20/1043-redes-sociales> [Consulta 15 Febrero].
- ✦ ROSE Karen, ELDRIDGE Scott, CHAPIN Lyman “*La Internet de las Cosas - una breve reseña*” Internet Society.org Octubre 2015 <https://www.internetsociety.org/wp-content/uploads/2017/09/report-InternetOfThings-20160817-es-1.pdf> [En línea] [Consulta 24 febrero 2019].
- ✦ SERRA URIBE, C.E: *Derecho a la intimidad y video vigilancia policial*. Madrid: Editorial Laberinto 2006.

♦ TORRES ROSELL, Nuria. Libertad vigilada y seguimiento continuado de penados: contenido e implicaciones político criminales. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2012, núm. 14-06 ISSN 1695-0194 Disponible en internet: <http://criminet.ugr.es/recpc/14/recpc14-06.pdf> [consulta 31 marzo 2019].

## LEGISLACION

♦ Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Publicado en «BOE» núm. 186, de 5 de agosto de 1997, páginas 23824 a 23828 (5 págs.) [En Línea] <https://www.boe.es/buscar/doc.php?id=BOE-A-1997-17574>

♦ Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Publicado en «BOE» núm. 93, de 19 de abril de 1999, páginas 14555 a 14561 (7 págs.) [En línea] <https://www.boe.es/buscar/doc.php?id=BOE-A-1999-8648>

♦ Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. Publicada en «BOE» núm. 252, de 17 de octubre de 2014, páginas 83921 a 84082 (162 págs.) [En Línea]. <https://www.boe.es/buscar/doc.php?id=BOE-A-2014-10517>

♦ Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia. Publicado en «BOE» 163 de 5 de Julio de 2014 [En línea] <https://www.boe.es/boe/dias/2014/07/05/pdfs/BOE-A-2014-7064.pdf>

♦ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Publicado en «BOE» núm. 294, de 06 de Diciembre de 2018. [En Línea] <https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

♦ Constitución Española de 6 de Diciembre de 1978. Publicado en «BOE» núm 311 de 29 de Diciembre de 1978 [En Línea] [http://noticias.juridicas.com/base\\_datos/Admin/constitucion.html](http://noticias.juridicas.com/base_datos/Admin/constitucion.html)

♦ MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES. Resolución de 28 de agosto de 2017, de la Subsecretaría, por la que se publica el Convenio entre el Ministerio de Defensa, la Secretaría General de Industria

y de la Pequeña y Mediana Empresa y el Centro para el Desarrollo Tecnológico Industrial, para coordinar las actividades de vigilancia y seguimiento espacial (SST - *Space Surveillance and Tracking*). Publicado en «BOE» núm. 216, de 8 de septiembre de 2017, páginas 89094 a 89102 (9 págs.) [En Línea] [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2017-10346](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-10346)

✦ Ley Orgánica 4/2015 de 30 de marzo de protección de la Seguridad Ciudadana Publicado en «BOE» núm. 77, de 31 de marzo de 2015, páginas 27216 a 27243 (28 págs.) [En línea] [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2015-3442](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3442)

✦ Ley Orgánica 2/1986 de 13 de marzo de Fuerzas y Cuerpos de Seguridad, publicada en «BOE» núm. 63, de 14 de marzo de 1986, vigente desde el 03 de abril de 1986 [en línea] <https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859>

✦ Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. Publicado en BOE de 29 de diciembre de 2017 [en línea] <https://www.boe.es/boe/dias/2017/12/29/pdfs/BOE-A-2017-15721.pdf>

✦ Tratados y Principios de las Naciones Unidas sobre el espacio Ultraterrestre, Naciones Unidas, Nueva York año 2002. [en línea] <http://www.unoosa.org/pdf/publications/STSPACE11S.pdf>

✦ Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia. «BOE» núm. 180, de 29 de julio de 2015 [en línea] <https://www.boe.es/buscar/pdf/2015/BOE-A-2015-8470-consolidado.pdf>

✦ Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal BOE» núm. 77, de 31 de marzo de 2015 [en línea] <https://www.boe.es/eli/es/lo/2015/03/30/1>

✦ REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de

datos) Diario Oficial de la Unión Europea [consulta en línea]  
<https://www.boe.es/doue/2016/119/L00001-00088.pdf>

❖ DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. Diario Oficial de la Unión Europea [consulta en línea]  
<https://www.boe.es/doue/2016/119/L00089-00131.pdf>

❖ Ley Orgánica 5/2010 de 22 de Junio por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Publicado en: BOE núm. 152, de 23 de junio de 2010, páginas 54811 a 54883 disponible en  
<https://www.boe.es/buscar/doc.php?id=BOE-A-2010-9953> [consulta 31 marzo 2019]

❖ DIRECTIVA 2002/58/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) Diario oficial de Comunidades Europeas disponible en <https://www.acave.travel/sites/default/files/comunitario-Directiva%202002-58-CE.pdf>

## **INTERNET**

❖ <https://www.blackbox.com.mx/mx-mx/page/23769/Recursos/News-Events/News/cmaras-analgicas-vs-cmaras-ip-una-comparativa-en-12puntos> [Consulta 9 Enero 2019]

❖ <https://www.xataka.com/privacidad/20-millones-de-camaras-equipadas-con-inteligencia-artificial-hacen-que-china-sea-el-verdadero-gran-hermano> [Consulta 10 Enero 2019]

❖ <http://www.milenio.com/tecnologia/chinos-seran-identificados-por-su-forma-de-caminar> [Consulta 14 Enero 2019]

❖ Wikipedia, la enciclopedia libre: [https://es.wikipedia.org/wiki/Cámara\\_IP](https://es.wikipedia.org/wiki/Cámara_IP) [Consulta 15 de Enero 2019]

- ❖Wikipedia, la enciclopedia libre:  
[https://es.wikipedia.org/wiki/Sistema\\_de\\_reconocimiento\\_facial](https://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial) [Consulta 9 de Enero 2019]
- ❖<https://www.telesurtv.net/news/tecnologia-china-sistema-de-vigilancia-reconocimiento-andar--20181105-0040.html> [Consulta 22 de Enero 2019]
- ❖<https://www.elperiodico.com/es/educacion/20180609/gran-hermano-colegios-china-camaras-reconocimiento-facial-concentracion-6868291> [Consulta 22 Enero 2019]
- ❖ <https://www.audio-technica.com/cms/site/9f3f5c571dcbded8/index.html> [Consulta 25 Enero 2019]
- ❖<https://www.espiamos.com/es/microfonos-espia-profesionales/> [Consulta 25 Enero 2019]
- ❖--<https://www.vistasur.com.ar/politica/seguridad-en-los-estadios-el-gobierno-estreno-un-sistema-de-seguridad-apuntando-a-la-vuelta-de-los-visitantes/> [Consulta 26 Enero 2019]
- ❖--<https://www.droneaviationcorp.com/solutions/wasp-aerostat> [Consulta 26 Enero 2019]
- ❖--<https://iiemd.com/drone/que-es-drone> [Consulta 26 Enero 2019]
- ❖--<https://www.unocero.com/ciencia/como-funciona-el-radar/> [Consulta 26 Enero]
- ❖--<http://elradar.50webs.com/aplicaciones.htm> [Consulta 26 Enero]
- ❖--<http://gabnav.coolinc.info/p3.htm> [Consulta 27 Enero]
- ❖--<https://www.youbioit.com/es/article/shared-information/15599/que-son-los-satelites-artificiales-y-como-funcionan> [Consulta 27 Enero]
- ❖—Periódico La Nación Digital <https://www.lanacion.com.ar/1912695-vigias-en-el-cielo-en-el-norte-habra-globos-aerostaticos-contras-el-narcotrafico> [Consulta 31 Enero 2019]
- ❖—Biblioteca Digital Chile <https://bibliotecadigital.indh.cl/handle/123456789/858> [Consulta 31 Enero 2019]
- ❖—<https://tableteduca.webnode.es/que-es-una-tableta-/> [Consulta 13 Febrero 2019]
- ❖—<http://culturacion.com/los-wearables-funcionan/> [Consulta 13 febrero 2019]

- ❖—Wikipedia, la enciclopedia libre [https://es.wikipedia.org/wiki/Local\\_Shared\\_Object](https://es.wikipedia.org/wiki/Local_Shared_Object) [consulta 23 febrero 2019]
- ❖—<http://www.allaboutcookies.org/es/faqs/balizas.html> [Consulta 23 febrero 2019]
- ❖—[https://es.ryte.com/wiki/P%C3%ADxel\\_de\\_Seguimiento](https://es.ryte.com/wiki/P%C3%ADxel_de_Seguimiento) [Consulta 23 febrero 2019]
- ❖—<https://www.cookiebot.com/es/website-tracking/> [Consulta 23 febrero]
- ❖—Wikipedia, la enciclopedia libre [en línea] <https://es.wikipedia.org/wiki/GPS> [consulta 11 marzo 2019] y <https://es.wikipedia.org/wiki/Compass> [consulta 14 de marzo 2019]
- ❖—<http://www.hablandodeciencia.com/articulos/2012/06/05/el-sistema-de-posicionamiento-global-gps/> [consulta 12 de marzo 2019]
- ❖—Artículo Redacción BBC Mundo. <https://www.bbc.com/mundo/noticias-41596292> [en línea] [consulta 14 de marzo 2019]
- ❖—useGalileo.eu - The Galileo device directory © 2019. <https://www.usegalileo.eu/accuracy-matters/ES> [en línea] [consulta 14 de marzo 2019]
- ❖—European Global Navigation Satellite Systems Agency “**Galileo**: el Sistema Global de Navegación por Satélite Europeo” <https://www.gsa.europa.eu/galileo-el-sistema-global-de-navegación-por-satélite-europeo>
- ❖—GOVERNMENT OF INDIA “ISRO” <https://www.isro.gov.in/spacecraft/satellite-navigation> [en línea] [consulta 16 de marzo 2019]
- ❖—<https://www.gps.gov/systems/gps/control/OCX/>
- ❖—GEO LOCALIZACIÓN <https://www.xataka.com/basics/que-es-y-cuanto-revela-de-tu-la-geolocalizacion-por-ip>
- ❖—“Localización y posicionamiento de móviles mediante antenas y GPS “ artículo web publicado 14 Noviembre 2017 por “jmesgon” [consulta 16 de marzo 2019] <https://gabinetejuridicotecnologicojuandemeseguer.es/localizacion-posicionamiento-moviles-mediante-sistemas-moviles-gps>
- ❖—MECAFENIX, Fran, Sensor Inercial o Sensor IMU. Publicación Web (23 Julio 2018) [consulta 18 marzo 2019] <https://www.ingmecafenix.com/automatizacion/sensores/sensor-inercial/>

- ❖—¿Qué es Zigbee? EfectoLED publicación web 19 abril 2018 [consulta 19 marzo 2019] <https://www.efectoled.com/blog/que-es-zigbee/>
- ❖—Blog BY. ¿que es RFID? [consulta 20 de marzo 2019] <https://www.by.com.es/blog/que-es-rfid/>
- ❖—Ultrasonidos [en línea] [consulta 23 marzo 2019] <https://definicion.de/ultrasonido/>  
<http://isbelg.over-blog.com/article-aparatos-ultrasonido-como-funcionan-para-que-sirven-86799573.html>
- ❖—Cómo localizar un dispositivo Bluetooth, por Pedro Delgado 14 septiembre 2015 [consulta 23 marzo 2019] <https://www.elgrupoinformatico.com/como-localizar-dispositivo-por-bluetooth-t25181.html>
- ❖—Localización WiFi, por José Antonio Barros, 27 Noviembre 2017 [en línea] [consulta 25 de marzo 2019] <http://www.compartirwifi.com/blog/localizacion-en-interiores-a-traves-de-tecnologias-como-wifi-o-beacon/>
- ❖—Localización WiFi, 11 febrero 2014, por Tartigues [en línea] [consulta 25 marzo 2019] <http://www.compartirwifi.com/blog/>
- ❖—GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR. Guardia Civil. Sistema SIVE [consulta en línea 27 de marzo 2019]
- ❖—GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR. APP ALERTCOPS [en línea, consulta 28 de Marzo 2019] <https://alertcops.ses.mir.es/mialertcops/>
- ❖— Derechos fundamentales afectados por la geo localización, artículo web de Juan de Dios Meseguer González disponible en <https://elderecho.com/derechos-fundamentales-afectados-por-la-geolocalizacion> [consulta en línea 31 de marzo 2019]

## 7. ACRÓNIMOS

**AESA:** Agencia Estatal de Seguridad Aérea

**APP:** Application

**BLE:** Bluetooth Low Energy

**GLONASS:** Global'naya Navigatsionnaya Sputnikovaya Sistema

**GSM:** Global System for Mobile Communications

**GPS:** Global Positioning System

**IoT:** Internet of Things

**IRNSS:** Indian Regional Navigation Satellite System

**LBS:** Location Based Services

**PRS:** Public Regulated Service

**RADAR:** Radio Detection and Ranging

**RFID:** Radio Frequency Identification

**RTLS:** Real Time Location System

**SIM:** Subscriber Identity Module

**SIVE:** Sistema Integrado de Vigilancia Exterior

**TIC:** Tecnologías de Información y Comunicación

**UE:** Unión Europea

**UWB:** Ultra Wide Band

**VANT:** Vehículo Aéreo No Tripulado

**VLC:** Visible Light Communication

**WiFi:** Wireless Fidelity (marca comercial)

**WALAN:** Wireless Local Area Network

## ANEXOS

En los anexos se muestran varias noticias de relevancia tecnológica. En ellas, se aprecia cómo las autoridades se han servido de los avances tecnológicos para el mejor desempeño de sus funciones y para conseguir resolver casos de actualidad que han mantenido a opinión pública en vilo.

En el anexo I es de interés destacar como se ha conseguido detectar sonido a través de un dispositivo móvil que reconoce las ondas sonoras del latido del corazón humano. Gracias a esto se ha conseguido detener una oleada de inmigración de personas que venían ocultas en un doble fondo de una embarcación.

En el anexo II se dan a conocer diferentes medios tecnológicos que vienen usando las Fuerzas de Seguridad destinados a labores de seguridad y control: sistemas informáticos, drones, robots y prototipos de coches patrulla dotados de videocámaras de control específicas (sin descartar que puedan incorporar visualización térmica o de infrarrojos, así como algún software de reconocimiento facial).

En el anexo III quiero mostrar cómo gracias a un dispositivo georradar, se pudo localizar la situación exacta en la que se hallaba el niño Julen, caído a un pozo de gran profundidad en Málaga, a principios de año. Esta maquinaria compleja fue necesaria para el mejor desempeño de los trabajos de rescate, en pozo de 100 metros de profundidad, situado en una finca de montaña.

En el anexo IV se muestra cómo se utiliza la tecnología de triangulación de telefonía celular. Ésta es muy demandada por las Fuerzas de Seguridad en casos como el de Diana Quer, en el que fue fundamental el uso de estas técnicas para la resolución de la investigación, pudiendo con ello hacer una reconstrucción que ha servido para desenmascarar al culpable.

## ANEXO I: SUCESOS INMIGRACIÓN

La Guardia Civil impide la entrada de 2.500 migrantes a buques atracados en Melilla.  
(EFEMadrid6 abr. 2019)



“Un dispositivo de la Guardia Civil establecido en el puerto de Melilla ha impedido desde el pasado mes de febrero la entrada a la península de 2.534 migrantes, de los que 76 eran menores de edad, cuyo objetivo era acceder a los buques como polizones.

Según ha apuntado el cuerpo en un comunicado, el dispositivo de seguridad en el puerto, que consta de dos anillos de seguridad -uno en la zona de tránsito público y otro en la interior, de acceso vedado- y vigilancia marítima.

En el anillo exterior, los agentes han empleado un dispositivo móvil que logra detectar latidos del corazón para evitar la entrada de personas ocultas en dobles fondos.

Las cifras de la Guardia Civil apuntan que el dispositivo ha logrado reducir en un 80 % la presencia de personas en la zona vedada, y en un 70 % la presencia de polizones con respecto a los datos del año pasado.

El dispositivo especial se desarrolla mientras se acometen obras de seguridad e impermeabilización en el puerto de Melilla, donde el pasado 15 de enero una persona falleció por aplastamiento en los bajos de una cabeza tractora en la que se había ocultado.”

Fuente EFE: <https://www.efe.com/efe/espana/sociedad/la-guardia-civil-impide-entrada-de-2-500-migrantes-a-buques-atracados-en-melilla/10004-3945938#>

## ANEXO II: LABORES HUMANITARIAS Y DE SEGURIDAD

Los grandes avances tecnológicos que ya aplica la Policía Nacional. En el Salón Internacional de Tecnologías de Seguridad Nacional, el cuerpo ha presentado sus nuevos equipos y un prototipo de coche policial que vigilará nuestras matrículas

Rodrigo Muñoz Beltrán (@RodrigoMBeltran Actualizado: 21/03/2017)



Actúan desde el aire con drones para salvar vidas, revisarán cada una de las matrículas y **podrán desactivar explosivos** sin que corra riesgo ninguna vida humana. La Policía Nacional ha presentado las novedades tecnológicas más importantes que ya utiliza en su labor diaria en HOMSEC, el sexto Salón Internacional de Tecnologías de Seguridad Nacional.

La Comisaría General de Extranjería y Fronteras cuenta con un avanzado sistema informático para controlar la inmigración. Está ya **instalado en los puertos y aeropuertos**, agiliza el control de fronteras y facilita el tránsito de personas.

Por el aire ya sobrevuelan los **drones policiales**. Empleados principalmente en labores humanitarias y como soporte de la policía científica. Según cuenta Francisco García, Inspector Jefe del Gabinete Técnico de la Policía Nacional, el dron se ha empleado recientemente en un rescate en las Islas Canarias. «Un joven **se cayó por un precipicio** y, gracias al dron, localizamos su ubicación y pudimos efectuar mejor el rescate. Fue todo un éxito», comenta orgulloso a ABC.

Los robots para desactivar explosivos ya existían. Sin embargo, la Policía ha mostrado su último modelo, el **AVANT-51**, que «ofrece más seguridad a los especialistas», e incluye más recursos tanto visuales (más cámaras para estudiar el **objeto sospechoso**) como para neutralizar posibles amenazas.

Aún no los podemos ver circular por nuestras calles, pero la Policía Nacional trabaja en un prototipo de coche patrulla. Lleva **dos cámaras instaladas en el techo del vehículo** y podrá controlar las matrículas de los coches. «Así resultará más sencillo detectar los automóviles sustraídos», comenta García.

«Si la sociedad evoluciona y aplica la más moderna tecnología, la Policía Nacional no puede quedarse atrás y también debe adaptarse a esas novedades», sentencia García. Porque, quizá, de esa evolución dependa nuestra seguridad.

Fuente: ABC digital: [https://www.abc.es/tecnologia/informatica/soluciones/abci-grandes-avances-tecnologicos-aplica-policia-nacional-201703190117\\_noticia.html](https://www.abc.es/tecnologia/informatica/soluciones/abci-grandes-avances-tecnologicos-aplica-policia-nacional-201703190117_noticia.html)

### ANEXO III: LOCALIZACIÓN

Los mineros paran a mitad de camino para localizar a Julen con un georradar. Técnicos señalan que usarán un tipo de georradar para localizar al pequeño antes de completar esta galería y poder ajustar mejor la excavación. Se han usado micro-voladuras para ablandar el terreno. (Javier Lerena Fran Extremera 25.01.2019)



Los mineros paran a mitad de camino para localizar a Julen con un georradar

Los ocho integrantes de la Brigada Central de Salvamento Minero han superado esta mañana la mitad del camino que les separa hasta el tapón bajo el que se encontraría Julen. Después de una noche bastante complicada, en la que especialistas en montaña de la Guardia Civil han tenido que realizar micro voladuras por la dureza del terreno, ya se ha superado la barrera de los dos metros de túnel horizontal.

De los aproximadamente cuatro metros que hay que excavar para alcanzar el pozo original, los mineros han alcanzado a las once de la mañana los 2,1 metros. Así lo han confirmado los técnicos que supervisan estas tareas de rescate y que avanzan que se está muy cerca ya de poder utilizar "un tipo de geo-radar" que permitirá localizar el lugar exacto en el que se encuentra el pequeño, "antes incluso de que se complete esta galería"

Fuente: Periódico digital [laopiniondemalaga.es](http://laopiniondemalaga.es) » [Málaga](#)

## ANEXO IV: LA INVESTIGACIÓN TECNOLÓGICA

El móvil atrapó a 'El Chicle'.

El cerco de La Guardia Civil sobre el asesinato de Diana Quer se estrechó a partir del rastreo de la víctima y del detenido. Reconstruyeron con 3D los itinerarios y el retrato robot del coche y con drones los escenarios. (Artículo de Carmen Jané, Barcelona - Martes, 02/01/2018 | Actualizado el 03/01/2018)



Efectivos de la UCO trasladan el pasado domingo a José Enrique Abuín, asesino confeso de Diana Quer. / **LAVANDEIRA JR (EFE)**

El **móvil** revela más de lo que parece y el '**caso Diana Quer**' ha vuelto a demostrarlo. La Guardia Civil **reconstruye las últimas horas de la chica** a partir del rastro dejado por el teléfono que iba manipulando (su último mensaje fue para lanzar un aviso sobre un hombre que la acosaba) en las antenas de telefonía, pero también fue esta la pieza que llevó hasta el detenido, José Enrique Abuín Gey, alias 'El Chicle', como presunto autor de su muerte.

El coronel jefe de la Unidad Central Operativa (UCO) de la Guardia Civil, Manuel Sánchez Corbí, explicó en la rueda de prensa celebrada este martes en A Coruña, que fue la velocidad de la señal del móvil de Diana lo que permitió determinar que la chica salió de A Pobra do Caramical en coche u otro vehículo motorizado y llegó a las 2.58 horas del 22 de agosto al puente de Taragoca, el mismo lugar donde apareció el móvil meses más tarde, cuando lo localizó un mariscador. Eso les ratificó en la tesis del secuestro.

Para cercar a 'El Chicle' fue necesario, según Sánchez Corbí, rastrear más de dos millones de datos recabados por las antenas de telefonía sobre los miles de personas que en la fiesta mayor visitaban la población. 'Big Data' en estado puro porque los policías piden a las operadoras "las conexiones de móviles en un rango amplio de horas y zonas" y estas les responden con un archivo de Excel. "Y encantados cuando se los das, aunque tienen traba-

jo para días", explican fuentes del sector. Este martes la Guardia Civil agradecía públicamente la información concedida y revelaba que "tuvieron que crear programas a medida para analizar la información", explicó.

#### De metros a kilómetros

Así, seguir un móvil sin GPS implica cruzar información de todas las antenas que captan su señal. A partir de tres se fija su posición con un margen de metros. Con solo una, el radio puede ser de hasta cinco kilómetros. La huella con la que se trabaja es el IMSI, un código internacional de 14 cifras que identifica el país, la operadora y el usuario de una red móvil, como el IMEI que identifica el terminal concreto, y se intenta contrastar que los datos coincidan para evitar que se aluda al cruce de tarjetas SIM y terminales.

‘El Chicle’ ofreció voluntariamente su móvil a los agentes de policía cuando le llamaron a declarar como testigo del caso Diana Quer en noviembre del 2016, pero no entregó a los agentes el que estaban buscando. Cuando se lo reclamaron, ofreció otro, pero con los datos "completamente reseteados. Explicó que se le había estropeado". A diferencia del IMEI, el IMSI no es accesible al usuario porque va encriptado.

#### Localizar el coche

Además del número de móvil, había que buscar otra certeza: el coche. Fue "frustrante", explicaron, peinar cámaras y radares de las carreteras de la zona para intentar localizar imágenes de la chica tras su desaparición. Cuando localizaron el móvil de Diana, un iPhone, no pudieron extraer los rastros del chip hasta que **intervino una empresa extranjera** que envió su informe en julio del 2017, cuando las diligencias del caso llevaban archivadas desde abril.

Con el informe obtuvieron la ruta definitiva del móvil hasta las 2.58, cuando se le pierde el rastro bajo el puente de Taragoca. Tras analizar las fotos de las cámaras llegaron a tres posibles vehículos sospechosos, de los que la Guardia Civil descartó uno, el otro llevaba remolque y el tercero era el coche de ‘El Chicle’.

Pidieron entonces ayuda a la empresa de análisis fotogramétricos ISV, una consultora de ingeniería con sede en Porrico especializada en la reconstrucción de accidentes, que ofreció el retrato robot del posible coche a partir de las "bolas de luz" que mostraban las fotos. "Trabajamos analizando las imágenes de las cámaras de seguridad de la autovía AG-11, y reconstruimos en 3D las posibles características del vehículo que se adaptaba a lo observado en las imágenes: marca, modelo y velocidad a la que iba", explica José A. Sabcedo, socio de la empresa.

Optaron por reconstruir los hechos. Cortaron la autovía AG-11 en pleno agosto y guardias civiles y técnicos midieron la ruta, las antenas y reconstruyeron en 3D el escenario. Las conclusiones de ISV excluyeron el remolque. Sus conclusiones las entregaron en un informe este mes de diciembre. "Han sido dos semanas de trabajo en laboratorio y dos meses para elaborar los informes judiciales", señala.

Técnicos de telefonía llegados desde Madrid aportaron otra pieza que faltaba en las averiguaciones policiales: porque el móvil de Diana y el del sospechoso seguían rutas distintas al entrar en la autovía. Y es que la telefonía GSM está diseñada de modo que en caso de saturación de terminales (A Pobra en fiestas), una antena distante puede captar el tráfico y por tanto aparecer la señal como más lejana de donde realmente está.

### Drones sobre los feriantes

La tecnología también ayuda a descartar hipótesis. Los agentes usaron imágenes grabadas con drones para ubicar los escenarios de las fiestas y dónde se alojaban los feriantes, un colectivo que en un primer momento estuvo bajo sospecha. "Su colaboración fue absoluta y sacamos un dato: uno de ellos reveló que había escuchado una discusión de pareja en aquella zona en aquella hora, lo que ratificó la tesis de que a Diana se la habían llevado por la fuerza", explicó el coronel Sánchez.

Para la Guardia Civil, poder disponer de los datos telefónicos ha sido clave. "En un momento en que en Bruselas se cuestiona si las operadoras han de conservar datos dos años, tenemos que decir que sin eso muchos casos no se resolverían", afirmó Sánchez, que reclamó que la medida siga en pie.

Hasta ahora, dijo, las antenas, el 3D y los drones han revelado el escenario. Lo que ocurrió más allá de las conexiones, cuando murió y cómo lo tendrán que decir los forenses.

Fuente: "El Periódico" edición digital

<https://www.elperiodico.com/es/sociedad/20180102/movil-clave-asesinato-diana-quer-6528065>